

{18+}

Даниил  
Туровский

Вторжение

Краткая  
история  
русских  
хакеров

1999-2009



@008044



*Моим родителям — за то, что научили любопытству*

Даниил Туровский

Вторжение.

Краткая история русских хакеров

Под редакцией Александра Горбачева

Издательство Individuum

Москва, 2019



## Предисловие

История русских хакеров — это история подростков всего бывшего СССР. Они росли в семьях советских инженеров, в юности читали киберпанк и научную фантастику, покупали на рынках клоны компьютеров IBM — и вдруг оказывались на хакерских форумах, которые часто заменяли им тоскливую русскую жизнь за окном: грязные улицы, бедность, пустое и пугающее в своей неопределенности будущее.

Пока в США рос экономический пузырь доткомов, хакеры запустили в России свою золотую лихорадку: воровство американских кредиток, взлом счетов банков и интернет-магазинов приносили многим миллионы долларов. Кто-то, боясь бандитов или государства, тщательно прятал их — вкладывая в цветочные магазины или пункты шиномонтажа; другие покупали особняки и дорогие спортивные машины; третьи обзаводились домами за границей и уезжали туда, где краски ярче, чем те, что они привыкли видеть за окном, — на Мальдивы, Кипр, в Израиль.

Биографии этих людей часто похожи на остросюжетные боевики. Когда я разговаривал с ними о прошлом, мне часто казалось, что все их проделки были не только ради денег — они как будто хотели стать героями книг и фильмов вроде тех, которые они так любили в детстве.

В юности я много читал журнал «Хакер», который то и дело советовал, как что-нибудь взломать, — все это напоминало обновленную для нового времени «Поваренную книгу анархиста». Я рос в семье, где у каждого был компьютер, а программирование приветствовалось; вечерами изучал коды сайтов — и пробовал их взламывать. В пятнадцать я раздумывал о том, чтобы пойти после школы учиться на факультет информационной безопасности — а потом, возможно, работать в ФСБ. К счастью, эти раздумья продлились недолго: вскоре я всерьез увлекся текстами, историями, журналистикой.

Тем не менее полутайное хакерское сообщество, попасть в которое мне так и не удалось, время от времени напоминало о себе. Сначала у знакомых взламывали соцсети и просили денег. Позже уже мои собственные аккаунты из-за работы репортером в России атаковали прогосударственные хакеры.

Эта книга про выбор — и про те пути, которые выбирали люди, которые стали частью хакерской субкультуры. Пока одни оставались романтиками и не думали о деньгах (часть I), другие богатели (часть II); когда пришло время устраивать отношения с государством, кто-то начал работать на него, а кто-то — против (части III и IV).

Книга основана на текстах, которые я в течение последних лет писал для «Медузы» ([meduza.io](https://meduza.io)), одного из немногих независимых российских изданий, но не ограничивается ими. Большую часть материалов я собирал в свободное от работы время, изучая форумы,

интернет-архивы, книги, встречаясь с хакерами или — чаще — разговаривая с ними в зашифрованных чатах. Я называю этих людей «русскими хакерами», потому что русскоязычное хакерское сообщество осталось единым: россияне, украинцы, белорусы и выходцы из других стран бывшего СССР росли на одних форумах, создавали совместные группировки и продолжали взламывать свои цели вместе, даже когда их государства вели друг с другом войну.

В чем-то эта книга — путеводитель по миру русскоязычных хакеров с последних лет СССР до нынешних времен; в чем-то — энциклопедия главных лиц; в чем-то — расследование о том, как российские власти построили одни из самых боеспособных кибервойск в мире. В книге много отдельных человеческих историй — по ним можно представить себе, в какой обстановке росли хакеры и что определило их дальнейшую судьбу.

В конце концов, это рассказ о том, как незнакомцы, сидящие за компьютерами, могут ссорить между собой страны, разрушать критическую инфраструктуру (например, отключать электричество в целых регионах) и убивать, не ведя при этом никаких боевых действий и не зная своих жертв.



## Пролог

### Первый беженец кибервойны

22 августа 2015 года бородатый мужчина в очках зашел с двумя рюкзаками в здание Ленинградского вокзала в Москве. Он прошел к кассам, где купил билет на ближайший «Сапсан» — поезд-экспресс, за 4 часа доезжающий до Санкт-Петербурга.

По прибытии мужчина поспешил к стоящим неподалеку от вокзала маршруткам. Он вырос в Петербурге и знал: микроавтобус до Хельсинки — самый дешевый и незаметный способ попасть из России в Европу. Билет стоит 800 рублей; путь занимает 8 часов, которые путешественник проводит в окружении бедных студентов и спекулянтов, везущих из России в Финляндию сигареты, а обратно — бытовую химию.

Через несколько часов мужчина перешел финскую границу и наконец немного выдохнул. Пока его план удавался: он наверняка сбросил хвост. Он все хорошо продумал: не полетел на самолете, потому что его бы задержали на паспортном контроле; билет на поезд покупал не в интернете, а прямо в кассе на вокзале. Мужчина вспомнил свой предыдущий побег из привычной жизни: десять лет назад он проезжал на троллейбусе мимо вокзала в Петербурге и спонтанно решил переехать в Москву к своей девушке. Вышел на следующей остановке, купил билет на поезд — и уехал на нем навсегда. С девушкой они потом поженились.

В Хельсинки мужчина сел на паром до Стокгольма, а в Швеции обратился к местным правозащитникам, попросив помочь с политическим убежищем. Те отправили его обратно в Финляндию: по европейскому законодательству просить убежище можно только в той стране, через которую человек въехал в Евросоюз.

Вернувшись в Хельсинки, бородатый мужчина нашел помещение с вай-фаем и написал письмо на общую редакционную почту «Медузы», где я работал специальным корреспондентом. Его почтовый адрес по-русски выглядел бы как «Мертваярука1984» — это отсылало одновременно и к антиутопии Джорджа Оруэлла, и к системе «Периметр», комплексу автоматического управления ответным ядерным ударом, созданному в СССР в разгар холодной войны. В Америке «Периметр» называли «Мертвой рукой»: система была придумана так, чтобы запустить ядерные бомбы, даже если все, кто мог это сделать вручную, к тому времени были бы убиты.

В письме мужчина представился Александром Вярей, одним из руководителей *Qrator Labs* — российской компании, занимающейся защитой от DDoS-атак [\*\*\*]. Он рассказал, что российские чиновники и спецслужбы интересуются кибероружием, а он сам был свидетелем того, как оно применялось по распоряжению государства.

«Сейчас, когда в РФ обстановка накаляется, я опасаясь, что меня могут „припахать“ заниматься организацией атак, так как я уже „в теме“, и я принял решение поставить общественность в известность, — писал Вяря (здесь и далее в цитатах героев сохранены ав-



торские особенности орфографии и пунктуации). — Я считаю, что граждане должны знать, на что тратятся деньги в условиях кризиса. И КТО занимается этими грязными делами. Это не какие-то мелкие жулики. Если раньше все только догадывались, то теперь у вас есть доказательства:) Чтобы меня внезапно не переехала машина, например, мне пришлось покинуть страну. Это решение мне далось очень нелегко, я, считай, потерял хорошую работу, уезжаю от семьи просто в никуда. Плюс сейчас всякие шлюхи вроде *Lifenews* будут меня „мочить“».

Я ответил, что хотел бы подробнее узнать его историю и встретиться лично. Наш разговор сразу же перешел в секретный чат в Telegram — в России 2015 года уже массово начали пользоваться защищенными чатами, понимая, что российские спецслужбы могут слушать и читать открытые каналы, хотя по закону и должны сначала получить на это разрешение суда.

— Как быстро вы сможете приехать? Собираюсь идти сдаваться и просить защиты, — написал Вря.

— Послезавтра?

— Оу.

— Долго?

— Нужно остановиться где-то сначала.

— Могу и завтра попробовать.

— Ох, я постараюсь найти какой-нибудь отель, у меня всего 4к на карте осталось.

Вря остановился в общей комнате одного из городских хостелов. Хельсинки — дорогой город, но ему повезло и он нашел ночлег за 20 евро в сутки. На следующее утро, когда я сидел в самолете, я получил от него сообщение: «Непередаваемый экспириенс с хостелом, я впервые. Храпят, говорят во сне, ворочаются всю ночь».

Вскоре мы встретились у торгового центра неподалеку от набережной. Вря стоял около дверей, нервно оборачиваясь и выглядывая меня среди переходящих через трамвайные пути. Все вещи — два рюкзака — были у него с собой. Мы зашли в ближайшее кафе, заказали кофе, и он начал рассказывать о том, что с ним произошло.

\*\*\*

Александр Вря родился в середине 1980-х в ленинградской коммуналке и рос без отца. Когда ему было двенадцать, он увлекся компьютерами — сначала видеоиграми, потом программированием и «железом». Первой его работой была должность системного администратора в компании его двоюродного дяди. Социальные сети тогда только начинали появляться, но аккаунты в них Вря не заводил принципиально: не хотел оставлять никаких следов в интернете.

Переехав в Москву, он поработал сетевым инженером в нескольких хостинг-компаниях [\*\*\*]. В 2012 году он обнаружил на одном из профильных форумов интересную вакансию — и после



пары тестовых заданий его взяли в компанию *Qrator*, специализирующуюся на защите от DDoS-атак.

К тому времени она уже лидировала на рынке: среди ее клиентов были и многие независимые СМИ (телеканал «Дождь», «Новая газета», «Ведомости»), и банки («Альфа», «Тинькофф»), и интернет-магазины («Юлмарт», *Lamoda*). По словам Вяри, их услугами даже однажды воспользовался интернет-магазин по продаже кедровых бочек; что удивительно — именно на него была совершена самая серьезная атака за все время его работы в компании. «В России популярно сводить счета с конкурентами с помощью DDoS-атак, некоторым магазинам один день простоя стоит закрытия», — объяснял он. Такие атаки стоят очень дешево (около 3 тысяч рублей в сутки) и могут при этом вывести незащищенный сайт из строя, что приведет к серьезным убыткам.

Вяря работал в техподдержке и постоянно отвечал на звонки клиентов. Нередко в *Qrator* обращались те, кто недоволен тем, что она защищает в том числе оппозиционные сайты. Весной 2012-го — накануне инаугурации президента Владимира Путина — прогосударственные хакеры-патриоты атаковали сайты «Эха Москвы», «Коммерсанта» и «Дождя» — все они были клиентами *Qrator*. «Зачем же вы защищаете евреев?» — сказал Вяре один из позвонивших в тот день.

Во время выборов мэра Москвы в 2013 году *Qrator* защищал сайт Алексея Навального: оппозиционный политик выдвинул свою кандидатуру и вел успешную кампанию. В какой-то момент Вяря заметил возле офиса компании фургон с тонированными стеклами и антеннами на крыше. В следующие дни он появлялся там почти каждый день. Выходя на обед, сотрудники *Qrator* пытались заглянуть в фургон и шутили, что тем, кто их прослушивает, надо бы принести пончики.

«Саша — талантливый человек, но очень впечатлительный и с тараканами в голове, — сказал мне его бывший начальник Александр Лямин. — Когда слишком долго работаешь в информационной безопасности, начинаешь меняться, начинаешь во всем видеть угрозу себе».

Так или иначе, к 2015 году Вярю повысили до руководителя службы эксплуатации. Он начал часто ездить за границу: приходилось посещать дата-центры, расположенные в европейских странах, чтобы устанавливать программное обеспечение, способное работать при больших нагрузках — во время атак. В *Qrator* такие серверы с фирменным ПО называют «центрами очистки трафика». Они помогают окружать сайты клиентов виртуальным «забором» с «пограничными пунктами», которые отфильтровывают здоровый трафик от паразитного.

Тогда же компания начала подготовку к открытию первого зарубежного отделения в Праге. Всем сотрудникам делали рабочие визы. Возглавить филиал должен был Вяря.



3 февраля 2015 года генеральному директору *Qrator* Александру Лямину позвонил Вартан Хачатуров, заместитель главы департамента инфраструктурных проектов Минкомсвязи. Хачатуров попросил кого-то из сотрудников компании помочь чиновникам с одним «щекотливым вопросом». Кроме Вяри помогать было некому: все разъехались по конференциям.

Хачатуров связался с Вярей и оставил номер телефона, на который тот отправил сообщение. Ближе к вечеру раздался звонок: звонил некий Василий Бровко. Вяря понятия не имел, кто это. Бровко сказал ему, что через пару дней им вместе необходимо слетать в столицу Болгарии, Софию; все необходимые документы оформит его помощница.

Вяря поискал в интернете информацию о Бровко и схватился за голову. Больше всего ему запомнилось, что тот основал компанию «Апостол», которую Алексей Навальный весной 2013 года обвинял в том, что она с помощью ботов [\*\*\*] раскручивала соцсети «Аэрофлота». В последнее время Бровко работал начальником департамента коммуникаций в «Ростехе» — госкорпорации, созданной для производства высокотехнологичной продукции гражданского и военного назначения. Руководил ею Сергей Чемезов, близкий знакомый Владимира Путина.

Вяря предположил, что от него хотят помощи по его профилю — выбрать новую систему защиты от DDoS. Но удивился, что позвали в Болгарию: известные производители соответствующего программного обеспечения находятся в Израиле и Штатах.

5 февраля 2015 года он прилетел в Софию. Отправил сообщение Бровко; тот ответил, что встреча состоится во второй половине дня. Вяря погулял по центру, потом подошел к назначенному месту — помпезному стеклянному зданию *Grand Hotel Sofia*.

Вскоре появился Бровко. В одной руке у него был смартфон российского производства, а в другой айфон; он постоянно что-то на них набирал. Вяря поприветствовал Бровко и сказал, что София — удивительно небольшой город. «Помойка», — бросил Бровко в ответ.

Следом появились двое мужчин. Они оказались сотрудниками местной компании *Packets Technologies* (сайт [1] компании скромно сообщает, что организация специализируется на «разработке передовых сетевых технологий»). Бровко сказал Вyre, что нужно сходить в офис компании: «посмотреть продукт» и высказать свое мнение.

Офис располагался неподалеку. В переговорной один из сотрудников *Packets Technologies* включил презентацию, а заодно рассказал о себе: работал в израильской армии, консультировал по сетевой безопасности крупнейшие интернет-компании, участвовал в *Black Hat* (главная мировая конференция по информационной безопасности, на которую приезжают и представители IT-корпораций, и хакеры).

После этого сотрудник болгарской компании, как утверждает Вяря, заявил: «Сейчас я вам представлю продукт для организации DDoS-атак». Названия у программного обеспечения не было. Сотруд-



ник добавил, что «продукт» умеет организовывать DDoS-атаки на сетевом уровне. Такие атаки «забивают» ресурсы сервера паразитными пакетами, из-за чего система перестает принимать полезные пакеты трафика.

Система представляла собой небольшое устройство — «коробку» с программным обеспечением, установленную на одном из трафикообменников [\*\*\*]. Для «продукта» была выделена специальная полоса с максимальной мощностью в 10 Гбит / с. Специалисты *Packets Technologies* добавили: система позволяет совершать «коктейльные» — то есть смешанные по типам — атаки, которые труднее всего отражать; кроме того, можно легко увеличить трафик, установив еще одну «коробку». В 2010 году атака силой 10 Гбит / секунду была совершена на серверы *Wikileaks*; мощность крупнейшей DDoS-атаки [2] в истории интернета — голландский хостер *Cyberbunker* против компании *Spamhaus* — достигала 300 Гбит / секунду: как писали в *The New York Times*, она «замедлила интернет».

Закончив с теоретической частью, сотрудник компании запустил VPN-соединение [\*\*\*] и Tor-браузер [\*\*\*], обеспечив себе анонимность (начало такой атаки отследить практически невозможно). Набрал в браузере IP-адрес [\*\*\*] — открылась страница с крайне простым интерфейсом. Наверху размещалась адресная строка, ниже — около десятка названий подвидов DDoS-атак, рядом с каждой — пустая ячейка, которую можно отметить галочкой. Внизу — кнопка для выбора мощности атаки: от 100 мегабит до 10 гигабит в секунду. «Можно не на всю катушку, если жертве достаточно поменьше», — поясняет Вяр.

Сотрудники компании ввели в строке интерфейса адрес сайта министерства обороны Украины. В соседнем окне открыли страницу сервиса, по которому можно определять работоспособность сайтов. Затем включили программу в полную силу. Возник график, показывающий мощность атаки — вскоре она достигла 10 Гбит / с. Сервис работоспособности показал, что сайт недоступен. Его попробовали открыть в браузере, но он не загрузился. Через пару минут атаку остановили и сайт снова стал открываться.

Потом они попробовали атаковать сайт украинского министерства обороны на мощности в 100 Мбит / с — он снова перестал работать.

«Давайте проверим на slon.ru», — предложил Бровко, до этого молчавший (я воспроизвожу его реплику со слов Вяри). «Слон» (сейчас называется *Republic*), одно из самых популярных независимых новостных СМИ в России, атаковали на мощности 10 Гбит / с. Сайт перестал открываться и лежал несколько минут. Позже тогдашний главный редактор «Слона» Максим Кашулинский подтвердил мне, что 5 февраля 2015 года они зафиксировали атаку, которая на две минуты обрушила сайт.

«А что, если сайты пользуются защитой? Пробьете?» — спросил Вяр. Ему ответили, что в этом случае придется узнавать реальный адрес сервера (все сервисы защиты пропускают атаку через себя, а



реальный адрес сервера маскируют), но у *Packet Technologies* есть соответствующая методика. Вяря уточнил, сколько стоит система; по его словам, Бровко ответил: «Около миллиона долларов».

После встречи Вяря и Бровко отправились в *Grand Hotel Sofia*. Сели в лобби, взяли кофе. Вяря вспоминает, что Бровко больше всего интересовало, как найти реальный адрес сайта и на каких трафикообменниках лучше всего ставить такую систему. Через некоторое время сотрудник «Ростеха» якобы сказал: «Ну что, нам нужен кто-то, кто будет этим управлять». Вяря поперхнулся и сказал: «Нет, извините. Я не хакер. Это против моих принципов, и это противозаконно». Бровко, по словам Вяри, спросил: «Ты знаешь, какая организация тебя сюда пригласила?» Вяря предположил, что он намекает на ФСБ, но вслух сказал, что впредь готов только отвечать на вопросы по технической части. Они добавили друг друга в *Telegram* и разошлись.

Вяря, по его словам, был шокирован произошедшим. Он сразу написал обо всем своему начальнику Лямину — тот рекомендовал «остаться максимально в стороне». На следующий день, 6 февраля, Вяря вернулся в Москву.

Вяря предоставил мне скриншоты дальнейших переписок с Бровко и свои с начальством. Сотруднику «Ростеха» он написал несколько сообщений с советами по технической части. В частности, порекомендовал использовать для системы голландские трафикообменники, где «проходят терабиты трафика — и на десяток гигабит не обратят внимания». Бровко ответил коротко: «Спасибо. Изучаю».

5 марта 2015 года Вяре написала помощница Бровко, сообщила, что тот просит о встрече: «На Патриарших прудах. Это не конкретное заведение, просто прогулка». Через несколько часов Вяря ответил, что этот вопрос нужно решать с его руководством. Тогда ему написал уже сам Бровко.

Привет. Мы же вроде договаривались иногда общаться без вовлечения твоего руководства.

Сможем сег повидаться?

Вяря:

Привет

шеф просит через него решить как он скажет

Бровко:

Нууу

Зачем?

Вяря:

он очень недоволен что через голову прыгают, обычно Вартан [Хачатуров] ему звонит и с ним обсуждает а я человек подневольный и без одобрения шефа не могу

Бровко:

Ну ты скажи, что кофе выпить выйдешь

Вяря:



к сожалению, не могу: (

Бровко:

Не прав, но ладно

Дай номер шефа своего

Лямину все это не понравилось. Он завел в *Telegram* чат под названием «WTF», куда пригласил Вярю, Бровко и Хачатурова.

Лямин:

Коллеги.

День добрый.

Сказать что я взбешен – это ничего не сказать.

Хачатуров:

Привет

Лямин:

Вартан, я всегда рад помочь тебе. Ты знаешь. Но когда к моим сотрудникам начинают лезть через мою голову – Я ПРОТИВ

Хачатуров:

Я честно говоря думал, что это разовая история:)

Лямин:

Я согласился помочь с Софией. Ни больше, ни меньше. Весь остальной «креатив» мной санкционирован не был. <...>.

Ждем комментариев и объяснений Василия Бровко.

Хачатуров:

Коллеги, давайте только спокойно:)

Лямин:

я спокойно в бешенстве

джентльмены так не поступают.

Бровко:

Не понимаю о чем речь в целом. Мне Денис [Вяря не знает, кто это такой. — *Прим. Авт.*] сказал, что вы мой консалтинг в очень щекотливом вопросе. Нет, так нет

Хачатуров:

Василий, просто Денис не сказал, что это длящаяся работа, а не разовая помощь:)

Бровко:

Разовая помощь

15 мин хотел

Хачатуров:

Мне кажется, это тогда не проблема, Саш

Лямин:

Я не знал что это 15 минут и зачем эти 15 минут

Хачатуров:

Просто нужно с тобой согласовать

Лямин:

В любом случае это мой сотрудник рабочее время которого оплачиваю я.

о чем вообще речь?

есть мой контакт – со мной и работайте.



дело не в том что 15 минут. дело в том что с людьми на моей зарплате общаются через мою голову. это недопустимо.

Хачатуров:

Ладно, Саш, успокойся, пожалуйста. Это недоразумение, и мы его уже урегулировали:)

Лямин:

Надеюсь меня услышали и поняли.

По словам Вяри, после этого Бровко и его сотрудники больше к нему не обращались.

\*\*\*

Я написал Василию Бровко на номер в *Telegram*, с которого тот предлагал Вяре встретиться для обсуждения кибератак. Он почти сразу же ответил, что «был в Болгарии для анализа системы защиты от киберугроз, а не для совершения таковых». «Не буду комментировать обвинения за рамками здравого смысла и не имеющие связи с реальностью, — добавил Бровко. — „Ростех“ постоянно подвергается кибератакам — с начала года на предприятия корпорации их было совершено свыше 11 тысяч».

Начальник Вяри Александр Лямин пригласил меня поговорить в офис *Qrator Labs*. Он оказался веселым разговорчивым бородачом в кедах и разноцветной футболке — и подтвердил, что Вяря ездил на встречу с Василием Бровко по просьбе Хачатурова из Минкомсвязи. «Речь шла вовсе не о системе для DDoS-атак, а о трафикогенераторе — системе, необходимой для проверки устойчивости сайтов к нагрузке, — сказал Лямин. — Да, скорее всего, был залп по „Слону“. Экспериментальный, на проверку. Нелегально? Это серая зона».

Лямин предположил, что Вяря чем-то обижен на его компанию и, возможно, рассказывая о заказе «Ростеха», выполнял заказ «Лаборатории Касперского», их главного конкурента. «В Финляндии доллары пригодятся», — сказал Лямин и отправил мне ссылку [3] на расследование *Reuters* о том, что Евгений Касперский призывал «мочить конкурентов». Он добавил, что не уверен, что Вяря «здоров».

Весной 2015 года сотрудников *Qrator* повсюду оформляли в Чехию. Вяря с семьей переехали из съемной квартиры в Чертанове в Бирюлево, чтобы немного сэкономить денег перед границей.

В конце мая Вяря обнаружил возле офиса знакомую машину — тот самый тонированный фургон с антеннами, который приезжал к зданию компании, когда *Qrator* обслуживал сайт Навального. Через несколько дней он увидел такой же автомобиль возле своего дома. Вяря говорит, что «начал параноить»: ему казалось, что он встречал одних и тех же людей в разных частях города. Он решил ездить из дома на работу разными маршрутами.

В последних числах июля Вяря сказал начальству, что не сможет ехать в Чехию, якобы потому что жена против. Тем не менее Лямин хотел, чтобы у сотрудников его компании были европейские



документы: он посоветовал Вяре получить вид на жительство в Финляндии, где у сотрудника были родственники по отцовской линии. Для ВНЖ требовалось сдать экзамен на знание финского языка. Вярю взял отпуск, чтобы его подучить.

Параллельно, по словам Вяри, его знакомые рассказывали, что им продолжают интересоваться сотрудники «Ростеха» и спецслужбы, чтобы в конце концов привлечь к работе над кибероружием, раз он уже видел его в действии. Вярю и сам был уверен, что так и произойдет — или его «ударят по башке».

В августе 2015 года друзья со связями в спецслужбах посоветовали ему покинуть Россию. На следующий день он собрал вещи в два рюкзака и уехал в Хельсинки.

\*\*\*

Ранним утром 25 августа 2015 года мы с Вярей пришли к полицейскому участку в Хельсинки, в котором он должен был заявить о том, что просит политическое убежище. Участок был еще закрыт; рядом ожидали несколько беженцев из Ирака. После короткого интервью и снятия отпечатков пальцев Вярю отправили в один из миграционных лагерей — трехэтажное здание недалеко от центра Хельсинки с бесплатной столовой. Внутри и вокруг дома ходили десятки иракцев и сирийцев, без остановки разговаривавших по телефону.

После заселения Вярю встретил беженца из Чечни. Тот рекомендовал ему беречь постиранные вещи: в лагере воруют. На следующий день он познакомился с парой из Сибири, скрывающейся от уголовного преследования, и интеллигентным сыном какого-то египетского министра. На третий день из лагеря увезли мужчину с подозрением на малярию. На четвертый день Вярю сказали, что после большого интервью с сотрудниками миграционной службы его, скорее всего, переведут в миграционный лагерь в 600 километрах к северу от Хельсинки — ждать решения по его делу.

Так и произошло. После этого в течение полутора лет Вярю переводили из одного лагеря в другой, периодически вызывая на дополнительные интервью. Его не сильно ограничивали в передвижениях; ему выплачивали пособие, на которое с трудом, но можно было жить.

Его историей заинтересовались в посольстве Украины в Финляндии — на встрече с украинцами Вярю рассказал, как проходила атака на сайт министерства обороны. «Ростех» и российские следственные органы на заявления Вяри никак официально не отреагировали.

\*\*\*

В конце декабря 2016 года на первой полосе *The New York Times* вышла заметка о Вярю, основанная на материалах, которые я делал для «Медузы» (позже газета получит Пулитцеровскую премию за серию материалов о России, включая этот). В тексте его называли



«элитным хакером». Вря удивился и написал мне: «Илитный хакир, блядь, что они несут?» После выхода статьи его в очередной раз вызвали на разговор финские спецслужбы — спросили, что он знает о российских хакерах и недавнем взломе энергетической системы Финляндии.

Летом 2017 года Вря наконец получил политическое убежище в Финляндии. В начале сентября — через два года после его бегства из России — мы решили встретиться. Я его не узнал. Он похудел на 20 килограмм и выглядел как человек, сбросивший груз, который его долго мучал.

Как рассказывал Вря, полтора года в финской миграционной системе дались ему непросто. Он даже пытался покончить с собой, но друзья вовремя вмешались и отвезли его в больницу, где он провел следующие несколько недель. Денег было мало, воссоединиться с семьей не получалось, допросы отнимали очень много времени; единственной отрадой была рыбалка, на которую он часто выезжал на велосипеде на целый день. Соседями Вря по миграционным центрам в основном были иракцы и сирийцы, бежавшие от «Исламского государства» (запрещено на территории РФ. — *Прим. ред.*). Большинство сидели на антидепрессантах, у многих были ранения. Они часто принимали Врю за сотрудника центра.

Купив пиво и травяную настойку, мы с Вряей дошли до одного из озер на окраине города: он где-то вычитал, что там хороший клев. «Я теперь уже как дома тут. Меня все устраивает, климат мой, — сказал программист. — Я будто и не в эмиграции уже, это моя новая жизнь». Открыв металлическую коробку и немного покопавшись в снастях, он закинул спиннинг в воду.

\*\*\*

Несколько недель спустя встречи с Вряей в одном из московских кафе я услышал знакомый голос. Обернувшись, я увидел бывшего начальника Вряи, Александра Лямина. Он давал кому-то интервью и сначала меня не узнал, а когда я поздоровался с ним, отвел глаза. Когда он уходил, я поздоровался с ним еще раз — оказалось, что, когда я поздоровался в первый раз, он подумал, что разговаривает слишком громко и мешает мне работать.

Лямин сказал, что рад, что Вряе удалось наконец получить документы. По его словам, большая часть сотрудников компании уже переехала в Прагу: оттуда удобнее предоставлять услуги по защите от кибератак. В конце разговора он спросил: «Что ты думаешь про историю с Михайловым, ФСБ, госизменой?» (незадолго до того высокопоставленный сотрудник ФСБ, занимавшийся киберпреступностью, был арестован по обвинению в государственной измене). Оказалось, Лямин в последнее время много об этом размышлял.

История Вряи — редкий случай, когда человек открыто рассказал об интересе российского государства и спецслужб к кибероружию. Возможно, Вря единственный, кто отказался работать над



таким оружием — и смог исчезнуть без серьезных последствий (если, конечно, не считать таковыми полный отказ от прежней жизни, в том числе семьи).

К осени 2017 года Вярä сменил имя и фамилию на финские; переехал, поменял телефон, почту и *Telegram*. Сейчас он мечтает купить большую лодку, с которой можно ловить лосося, ходящего на большой глубине. Похожими вещами он занимается и на работе: он устроился в неправительственную организацию, которая следит за тем, как одни государства совершают кибератаки на другие.



# Часть I

## Корни

### Глава 1

#### Территория свободы

В 1992 году молодой житель Санкт-Петербурга Кирилл впервые попал [4] на рынок «Юнона» на юго-западной окраине города. Сформировалась толкучка еще в предыдущем десятилетии: вокруг магазина «Юный техник» собирались люди, которые продавали радиодетали, разложив их на тротуарах. С наступлением рыночной эпохи рядом отгородили территорию и поставили прилавки — при этом рынок сохранил свою специализацию: в основном там торговали электроникой и запчастями к ней. Одними из популярных предложений были 15-минутные сеансы игры на приставке *Atari*.

Как и многие петербуржцы, Кирилл купил на этом рынке свой первый компьютер — и сразу начал проводить за ним много времени. Через пару лет юноша ненадолго уехал в США, где как раз начал приобретать популярность интернет; в Калифорнии Кирилл открыл свой первый браузер. Вернувшись на родину, он заметил, что свой цифровой андеграунд постепенно зарождается и в России, и решил делиться с людьми полученными в США знаниями про то, что такое WWW, FTP [\*\*\*] и IRC [\*\*\*].

Вскоре Кирилл познакомился с другими первыми российскими любителями компьютеров и интернета. Себя они называли «сценой», их было около 30 человек, большинство жили в Москве и Петербурге. В 1995 году они впервые собрались на *Enlight*, фестивале любителей компьютеров; среди прочего там, например, проводился конкурс по метанию винчестера на дальность. Впрочем, в основном они встречали друг друга в IRC-чатах — и это общение многим заменяло обычное.

«Улицы России тогда были куда менее приветливыми, чем сегодня. Самой популярной темой для разговоров всегда была сама жизнь. Всё — от баб до космоса», — рассказывал один из представителей «сцены». — «Конкретных тем не было, фан заключался в том, что мы стали первыми в мире, кто использовал преимущества интернета для общения. Когда [в 1997 году] принцесса Диана разбилась — это произошло ночью, — на канале были люди отовсюду. И один из них жил в квартале от происшествия. Он сходил, посмотрел и, вернувшись, стал рассказывать о своих впечатлениях. А весь мир начал это обсуждать только через 8 часов, просмотрев выпуски новостей».

Одной из главных проблем в те годы было получить доступ к компьютеру: иногда это было непросто даже для тех, у кого они были дома. Программист Антон Мельников подробно вспоминал [5], на какие ухищрения ему и его другу Мише приходилось идти, чтобы



играть в компьютерные игры, — например, прогуливать школу. Вначале они симулировали болезни и печатали справки на струйном принтере. «„Болезнь“ дома я не мог, так как у нас жила бабушка, поэтому каждое утро приходилось мучительно вставать и переться как будто бы в школу. Иногда врал, что нужно ко второму-третьему уроку, но часто так делать было нельзя — палево, — рассказывал Мельников. — Вместо школы я шел к Мише, но была проблема: его дом был ровно напротив школы. Так как в этот момент все одноклассники и учителя тоже шли в школу, приходилось играть в шпиона: идти аккуратно, нарезать круги, прятаться за сугробами etc. Потом пасти, когда отец Миши свалит на работу».

Были и другие трудности. «Отец Миши увидел появляющуюся у него зависимость [от игр и интернета] и собрал чудо-девайс, который подавал электричество на комп только при наличии ключа, — вспоминает Мельников. — Миша ключ, конечно, спиздил и сделал копию». Когда отец друга, как-то вернувшись домой, обнаружил, что монитор горячий, он начал прятать провод питания — и тогда подростки купили замену. Потом отец Миши стал убирать монитор в кладовку. «Но и тут решение было найдено. У двери были большие зазоры, и мы просто научились снимать ее с петель, — продолжает Мельников. — Самая жесть случалась, когда кто-то звонил в дверь. Нужно было оперативно отключить монитор, оттащить его в кладовку и поставить дверь на место».

В итоге друзья прогуляли почти целую школьную четверть. «Разоблачение закончилось одним из самых стыдных моментов в моей жизни, — говорит Мельников. — Нас шеймили перед всем классом. И каждый следующий учитель делал это заново. Особенно их тронула подделка справок. Нам пророчили карьеру фальшивомонетчиков». Теперь он играл у себя дома по ночам, разработав сложную систему, которая отключала систему охлаждения компьютера, чтобы он не шумел и не вызывал подозрения у родителей. Недостаток у нее был один: техника перегревалась — и однажды Мельников проснулся от того, что в комнате стоял запах гари.

Только через некоторое время после этого у подростков появился доступ в сеть. «Платить за интернет на фоне моей опустившейся школьной успеваемости никто не хотел, но выход нашелся, — говорит Мельников. — У провайдера „Метаком“ появился „гостевой доступ“. Халявный пул, где можно было посидеть в местном IRC и поюзать фтп. Время не было ограничено, но было очень сложно дозвониться. Хочется сказать спасибо людям, которые это сделали. Они во многом изменили мою судьбу и помогли найти себя на долгие годы. В общем, сидел я там безвылазно. Обзаводился друзьями и развивался как айтишник».

Похожим образом были устроены жизни и других молодых россиян, открывших для себя компьютеры. Некоторые из них быстро поняли, что на этом можно еще и зарабатывать: тем более что, как вспоминает Кирилл, большинство первых хакеров увлекались во-



шедшими тогда в моду рейвами и наркотиками, на которые нужны были деньги.

По словам хакера, сначала «сценеры» занимались «варезом» — компьютерным пиратством. Другие тратили дни (с медленным интернетом того времени), чтобы скачать популярные программы, записывали на CD-диски и перепродавали на рынках.

Следующим этапом стало воровство кредиток и взломы закрытых сетей — это приносило куда больше денег, чем пиратство. Участники группировки STEALTH рассказывали [6], что еще в 1994 году внедрились в американское посольство и называли себя «создателями боевых роботов-убийц на просторах киберпространства». Их коллеги вспоминали [7], как взламывали сайт Новороссийска и получали доступ к компьютерам Верховной Рады Украины. Сам Кирилл в какой-то момент основал хакерскую группировку *Sodom*. Ее лозунг гласил: «*Russian Mafia — we'll take care of you*».

«В девяностых Россия и Украина зажигали по полной. Можно было делать все что угодно, так как не было никакой законодательной базы, — вспоминал участник хакерского андерграунда начала 1990-х. — Нашей свободе завидовали все. В России не было ограничений, как у ребят в Европе и Штатах. На мировой сцене нас всегда уважали и боялись, так как подрастающему поколению парни из России внушали животный страх рассказами о пушках, водке, мрачных улицах и других вещах».



## Глава 2

### Как обидеть тетю Асю

Это наш мир, мир кодов и электронных импульсов, наполненный красотой модных звуков. Мы бесплатно пользуемся услугами, которые могли бы стоить копейки, если бы вы не спекулировали на наших потребностях и не были так жадны, – вы называете нас преступниками. Мы стремимся к знаниям – вы называете нас преступниками. Мы существуем без цвета кожи, без национальности и религиозных предубеждений – вы называете нас преступниками. Вы производите атомные бомбы, разжигаете войны, убиваете, обворовываете и врите нам, пытаетесь убедить в своей правоте, – а мы все так же остаемся преступниками. Да, я преступник. Мое преступление – любопытство. Мое преступление – в том, что я сужу о людях по их знаниям, мыслям и поступкам, а не по тому, как они выглядят. Мое преступление в том, что я умнее вас, за что вы не можете меня простить. Я хакер, и это мой манифест. Вы можете остановить кого-то из нас, но вы не можете остановить нас всех.

В 2003 году в российском издании «Хакер» был опубликован [8] фрагмент манифеста хакеров, который впервые появился за 17 лет до того в американском сетевом издании PHRACK. Для читателей русского перевода все сказанное в нем уже было прописными истинами: к тому моменту издание для «компьютерных хулиганов» пять лет весело и доступно рассказывало всем желающим, как взламывать электронную почту, организовывать DDoS-атаки и воровать данные кредитных карт.

«Хакер», запущенный в 1998 году издательским домом *Gameland* (в основном там выходили журналы о видеоиграх), быстро стал для многих российских школьников и студентов предметом своего рода культа. Этот ежемесячный журнал чем-то напоминал «Поваренную книгу анархиста» Уильяма Пауэлла. В начале 1970-х молодой и злой Пауэлл, считавший, что знания должны быть доступны всем, а люди способны сами принять разумные решения, написал и издал пособие, в котором рассказывалось, как делать взрывчатку из общедоступных ингредиентов, вести слежку и убивать людей. На протяжении следующих десятилетий книгу нередко находили в квартирах террористов и убийц – например, подростков, устроивших стрельбу в американской школе «Колумбайн» (сам Пауэлл в итоге стал учителем и многие годы пытался запретить переиздавать свой труд).

В первом же номере «Хакера» была опубликована инструкция о взломе кредитных карт; во втором – советы о том, как угнать аккаунт в мессенджере ICQ (заголовок: «Как обидеть или защитить тетю Асю»), а также материал с перечнем программ для взломов. «На самом деле существует два способа хакать, – писал автор материа-



ла. — Первый: ты покупаешь кучу книг по устройству и работе Интернета, языкам программирования, операционным системам, протоколам, работе процессора и т. д. Ты все это внимательно читаешь и через два года тренировок сможешь видеть все дырки и получать нужную тебе инфу без проблем. Но ведь ты лентяй! <...> И поэтому ты выбираешь второй способ: пусть другие парни книжки читают и программы пишут, а я уже воспользуюсь плодами их труда. Ну что ж, ладно, хорошо, не вопрос!»

В других материалах журнала рассказывалось про «самые урожайные хаки» и про места в интернете, где можно искать уязвимости нулевого дня [\*\*\*]. Журнал публиковал мемуары человека, взломавшего банк; советы, как не попасться в лапы к спецслужбам; и интервью со знаменитостями — певец Дельфин, например, называл хакерство «экстремальным видом спорта» и признавался, что и сам хотел бы «что-нибудь взломать».

В шестом номере «Хакер», рассказывая об уязвимостях критической инфраструктуры, даже нечаянно предсказал будущее своих читателей. «Информационные войны в конце XX века стали настолько реальными, что в определенный момент можно будет развернуть третью мировую, не выходя из дома, сидя за клавишей своего компьютера, — писал автор материала. — И если раньше министерствам обороны различных стран приходилось уделять особое внимание защите своих наземных, воздушных и морских границ, то теперь появилась еще одна граница — виртуальная. Ну и кто же эти границы будет защищать? На мой взгляд, это будут выросшие хакеры, которым надоест заниматься всякой шнягой бесплатно, и они применят свои знания для работы на спецслужбы и Министерство обороны, становясь виртуальными пограничниками, отслеживающими каждый электрон, проходящий от континента к континенту».

Журнал фактически предлагал российским подросткам, жившим в бедных провинциальных городах, где нечем заняться, альтернативу. «Тебе катастрофически не дают. Обидно, но это легко исправить — стань хакером», — прямо говорилось в одном из номеров. Будущий хакер, который в 2000-х начал заниматься кардингом, в конце 1990-х рос в сибирском городе: в советское время он был организован вокруг большого промышленного предприятия, но после распада СССР завод закрылся и большинство жителей лишились работы. Раз в месяц после школы подросток ходил в единственную в городе палатку с прессой и покупал новый номер «Хакера» — продавщица в какой-то момент начала узнавать его в лицо и сразу протягивала ему журнал. «Возможно, к нам вообще только один номер и привозили, — вспоминал хакер в разговоре со мной. — Как бы тупо это ни звучало, „Хакер“ был как глоток свежего воздуха среди общей серости вокруг».

Впрочем, читали «Хакер» и в Москве. Илья Гофман родился в конце 1970-х в интеллигентной семье: его отец был композитором, мать занималась искусством. В детстве у него была сильная аллергия и астма, из-за чего он учился дома. У мальчика обнаружился та-



лант и к музыке — он играл на скрипке и альте, — и к математике: он увлекался алгеброй и в подростковом возрасте опубликовал несколько научных работ в математических журналах. После школы Гофман поступил в Московскую консерваторию имени Чайковского — одним из его преподавателей стал Юрий Башмет. К концу 1990-х Гофман считался [9] одним из самых перспективных и талантливых российских академических музыкантов.

Весной 1998 года он увлекся журналом «Хакер». Больше всего Гофману нравилась рубрика «Взлом», в которой рассказывалась, как воровать данные кредитных карт и преодолевать защиту банков; как он позже говорил, «все [было] доступно, как в сказке». Хакерство казалось юноше «удивительным явлением из области человеческого воображения», занятием романтического толка. «Одно дело — человек играет в компьютерную игру и не может из нее вылезти, — объяснял Гофман позже. — Но это понятно — потому что игра красивая, разработан интерфейс. А хакер живет в виртуальном мире, но имеется в виду не компьютерная реальность, а его внутренний мир. Это человек, который видит черный экран и мигающий курсор — и этого достаточно для него, чтобы он понимал, что он в этот момент действительно там. Это было как ребус, было довольно забавно изучать. Это была очередная математическая задача, да, на грани, но никто не ставил целью никакие финансовые операции. Мне казалось, что мораль не нарушается. Ведь у всего этого в банковской системе есть компенсационные механизмы — все восстановимо».

Он взял себе ник *NetSerpent* («Интернет-змея») и нашел компаньонов. Вместе они смогли перевести на свои счета около 97 тысяч долларов из 16 американских банков и нескольких российских: информацию о картах получили после взлома канадского интернет-магазина. Подозрительную активность заметили сотрудники отдела безопасности российского банка, в котором эти счета находились. Искать злоумышленников долго не пришлось: все счета они открывали под своими настоящими именами.

На украденные деньги хакеры покупали сотовые телефоны (тогда они были роскошью), а также вещи из бутиков *Versace* и *Calvin Klein*. Гофман свою долю потратить так и не успел: осенью 1998 года всех задержали и юного скрипача как предполагаемого организатора группировки отправили в СИЗО. В «Московском комсомольце» их называли [10] «змеями из интернета».

В защиту Гофмана выступил Юрий Башмет, который назвал его «не только одним из лучших студентов моего класса, но и одним из лучших молодых альтистов Москвы». «Мне кажется, что необходимо сделать все возможное, чтобы сохранить его талант для нашей отечественной культуры», — говорил музыкант. Несмотря на это (и на астму), Гофман полгода просидел в «Матросской тишине» в камере на 70 заключенных — где продолжал писать музыку.

Суд приговорил юного москвича и его подельников к пяти годам условно. Выйдя на свободу, Гофман стал лауреатом IV Между-



народного конкурса альтистов Юрия Башмета и продолжил музыкальную карьеру, выиграв еще несколько мировых соревнований альтистов. Сейчас он преподает в Гнесинке и часто выступает с концертами.



## Глава 3

### Сомнения стали страстью

На первых российских хакеров влияли не только форумы и профильная пресса, но и поп-культура. О людях, которые, сидя за компьютерами, управляют судьбами и государствами, писали фантасты и снимали фильмы в Голливуде. Первый из них появился еще в 1983 году — он назывался *Wargames*, и один из хакеров, взламывавший предприятия по всему миру в поисках секретных документов, рассказывал мне, что в детстве кино произвело на него большое впечатление. По сюжету хакер-подросток, проникнув в сеть американского военного ведомства, находит там файлы, которые принимает за видеоигры: «Воздушные бои», «Военные действия в городских условиях», «Война в пустыне», «Глобальная термоядерная война». В итоге дело чуть не заканчивается третьей мировой. Когда *Wargames* только вышел, он всерьез напугал [\[11\]](#) тогдашнего президента США Рональда Рейгана — после этого Рейган поручил разработать стратегию национальной безопасности в области автоматических информационных систем; секретная директива об этом была подписана в 1984-м.

В середине 1990-х Голливуд снова обратился к теме хакеров. Один из фильмов, который так и назывался — «Хакеры», запустил карьеру Анджелины Джоли и рассказывал о том, как группа киберподпольщиков борется с алчным сотрудником транснациональной корпорации. Когда в 2004 году был проведен большой опрос [\[12\]](#) среди посетителей русскоязычных хакерских форумов, выяснилось, что именно это кино повлияло на них сильнее всего, заставив задуматься о самоидентификации и «сопротивлении корпоративной глобализации».

До России видеокассеты с «Хакерами» добрались почти одновременно с тем, как фантаст Сергей Лукьяненко написал свой роман «Лабиринт отражений» о «дайверах», работающих в виртуальных мирах. При всем киберпанке во многом книга была реалистичной: в перерывах между рейдами в интернет герой ел бутерброды с колбасой. В романе даже был романтический гимн хакеров:

Наша работа во тьме —  
Мы делаем, что умеем,  
Мы отдаем, что имеем, —  
Наша работа — во тьме.  
Сомнения стали страстью,  
А страсть стала судьбой.  
Все остальное — искусство  
В безумии быть собой.

Несколько моих собеседников рассказывали, что хорошо помнят этот диссонанс между повседневной российской реальностью 1990-х, когда даже на колбасу хватало не у всех, и безграничными возможностями интернета. К концу десятилетия на многочислен-



ных хакерских форумах уже сложилось крепкое сообщество со своей атмосферой и даже своей культурой: кто-то сочинял стихи, кто-то — рассказы. Писали и «секретные инструкции для хакеров» о том, как выглядеть классно, если тебя снимают журналисты. Одна из них выглядела так:

- 1) Сесть за любое устройство, имеющее экран и клавиатуру
- 2) Надеть очки
- 3) Попросить взглядом оператора повернуть камеру, чтобы экран отражался в очках
- 4) Тыкнуть любую кнопку, чтобы появилась полноэкранная программа взлома пентагона, со специальными индикаторами уровня и прогресса взлома.
- 5) Заебашить лук самого ниипического IT-GOD-а
- 6) Перемять или хрустнуть пальцами
- 7) Начать клацать всеми 10-пальцами со скоростью света по клавиатуре без Энтера и Пробела в течении 10 сек.
- 8) Приостановиться на пару сек и сказать нас засекли
- 9) Заклацать опять по клавe со скоростью света X2, чтобы опередить тот брандмауер [\*\*\*], который засек.
- 10) Откинуться назад и сказать: вот так вот Епта, ай Эм Год
- 11) Перевести себе 99999999999999999999999999999999 \$\$\$
- 12) 5 лет учебы на ИТ-шика оправдали себя \ . ...

Возникали на хакерских форумах и более сложные творческие проекты. В конце 1999 года там начала распространяться пьеса [13] «История, которой не было, или Хакнутые выборы-99». Ее героями были одни из самых активных хакеров тех лет, а рассказывала она о том, как они взламывают российскую избирательную систему:

```
MeteO> дело есть. на много баксов.  
Leshy> а сколько лет за это могут дать?;)MeteO> тебе-то уж точно вышка светит =)  
Leshy> ну, рассказывай...MeteO> в общем, ты наверное в курсе, что скоро выборы? Leshy> угу.. «Яблоко» – рулез!MeteO> никакой оно не рулез.;) в общем, ты знаешь, как устроена ГАС «Выборы»?Leshy> в принципе да. Дерьмо полное. Ты что, поломать ее удумал?MeteO> однако ты у нас сегодня еще и догадливый?! =)
```

<...>

```
Leshy> Ясно. чей заказ?MeteO> Березовского.Leshy> Е$бнулся, Путина и этих $%^; № % Шойгу, Гурова и Карелина проталкивать?MeteO> Не ерепенься. Мы параллельно с людьми Гусинского контактировали – они тоже не прочь раскошелиться =)Leshy> Мне не хочется в лучшем случае на костылях оставшуюся жизнь ковылять...MeteO> Ну и паникер же ты... =)
```

Ближе к финалу в пьесе возникал сюжет из аналитической программы, которую тогда вел на ОРТ (сейчас — Первый канал) Сергей Доренко. «Как нам стало известно из источников, близких к ЦИКу и



ФСБ, есть вероятность того, что в систему ГАС „Выборы“ проникла группа хакеров, — рассказывал ведущий. — Как вы видите на табло в Федеральном Информационном Центре „Выборы-99“, находящемся в Останкино, график предпочтений избирателей закономерно скачет — то на 5 % вырастает рейтинг у „Единства“, то у „Яблока“».

После этого по сюжету начинались беспорядки: «Народ уже вовсю бесновался. По многим каналам транслировали то, как уже в закрытых избирательных участках происходили драки, спровоцированные нервными сторонниками какой-то из политических сил, и народ в буквальном смысле разрывал бюллетени при вскрытии корзины с ними. В общем, началась повальная паника и беспредел».

Тогда такие сюжеты посетители хакерских форумов могли только выдумывать. Через двадцать лет — в 2016 году на президентских выборах в США — их мечты станут реальностью.



## Глава 4

### Школьники взламывают NASA

Большинство хакеров поначалу занимались взломами для развлечения: воровали пароли от родительских компьютеров, ломали соседский интернет, угоняли ICQ у друзей. Как сказал один из моих собеседников, «оказалось, что от воровства ICQ до участия в информационных войнах не так много шагов».

«[В середине 1990-х] интернет охватил все регионы России и принял глобальный характер. О проделках так называемых хакеров можно было услышать только из-за бугра или увидеть в кино, но наши люди не заставили долго ждать, — вспоминал [14] один из хакеров, начинавший в те годы. — Вскоре в России был организован отдел по борьбе с компьютерными преступлениями, в московских газетах появились статьи о „маленьких гениях-хакерах“, которые теперь отсиживают срок. На самом деле были пойманы бедные детки, студенты, которые просто хотели подзаработать немного денег через интернет, заказывая товар на дом по фальшивым кредиткам (к реальному хакерству это ну никак нельзя было отнести). А тем временем, пока люди из ФСБ гонялись за этими „хакерами“, другие спокойно себе сидели дома и получали новые знания, чувствуя себя в полной безопасности. Можно даже сказать, что хакерство в России развивалось с огромной скоростью и при этом не ощущало никаких преград со стороны органов правопорядка».

В 1998 году несколько приятелей создали группировку под названием «Камера предварительного заключения» — чаще они сами себя называли KPZ. «Как раз тогда тысячи подростков, посмотрев дошедший до России фильм „Хакеры“ и начитавшись статей в журналах, ринулись в интернет, возомнив себя профессиональными взломщиками», — вспоминал [15] участник группировки. В KPZ состояли от пяти до десяти участников. Первым делом они отомстили известному московскому компьютерному клубу «Орки», администрация которого «нанесла некоторый моральный ущерб» одному из друзей. Группировка взломала серверы заведения. После этого KPZ выполнила несколько взломов на заказ, а когда в российском интернете «ничего привлекательного не осталось», заинтересовалась интернет-ресурсами правительства США. Как утверждали [16] участники группы в одном из номеров «Хакера», они сумели взломать [17] 21 американский сайт — среди них были ресурсы университетов, военных ведомств и NASA.

Хакеры из KPZ довольно охотно рассказывали о себе — один из них признавался, что ему 15 лет и он учится в 10 классе. «Можно сказать, что я — хорошист:) Учусь на 3-4, — писал [18] он в материале, опубликованном в «Хакере» в 1999 году. — Кстати, в нашей школе даже нет предмета „Информатика“. Вот такая вот школа:) Приходится все познавать самому: читать много книг на любые компьютерные темы, экспериментировать и делать многое другое без какой-либо помощи окружающих. В недалеком будущем собираюсь



пойти работать в техподдержку к какому-нибудь провайдеру. Ну и было время, что мы нахацкали кучу военных хостов».

Как-то раз в квартире одного из участников KPZ выключилось электричество. В дверь постучали.

— Кто там? — спросил хакер

— Милиция! Откройте.

— По какому поводу?

— По компьютерному.

Войдя в квартиру, милиционеры забрали компьютер и повезли участника группировки в свой участок. Там они открыли на компьютере ICQ, изучили его, но «увидели только загадочные слова». Задав юноше несколько протокольных вопросов — «они даже и не знали, что спрашивать», — милиционеры отпустили его домой.

С развитием хакерского сообщества постепенно начал формироваться и рынок, на котором можно было купить их услуги. Дмитрий (имя изменено по его просьбе) заинтересовался взломами в начале 2000-х, когда ему было 13: для игр его компьютер был недостаточно мощным, а заняться чем-нибудь хотелось. Сначала они с одноклассником делали сайты: друг рисовал дизайн в тетради на уроках, а Дмитрий прямо на бумаге писал код. «Такие ограничения способствовали изобретательности, и у меня довольно быстро возник интерес к тому, как такие сайты ломать», — вспоминает хакер.

Первыми его жертвами стали сайты других школьников. Вскоре он открыл для себя хакерские форумы. Тогда их было много: `hackzone.ru`, из которого потом вырос закрытый *Underground Information Center* (старожилам *Hackzone* не нравилось, что сайт заполнили подростки, и они решили создать для себя отдельное пространство), `bugtraq.ru`, `void.ru`. Дмитрий стал завсегдатаем «Античата» [19], где обсуждались компьютерные уязвимости, взломы и новости информационной безопасности. Как и в случае других форумов, многие посетители «Античата» фактически жили на сайте — и даже посвящали ему песни [20]:

Просыпаясь рано утром, я включаю интернет  
Захожу на `Antichat.ru`, в мире сайта лучше нет...`Античат.ру`,  
`Античат.ру`, За тебя я все сайты перетру!`Античат.ру`,  
`Античат.ру`, Потому что я тебя люблю

На форуме было несколько уровней доступа; попасть на следующий можно было, написав статью и доказав свои познания в программировании. Поднимаясь вверх в иерархии «Античата», Дмитрий познакомился с другими молодыми хакерами. Несколько лет спустя многие из них станут лучшими в России специалистами по кибербезопасности; другие начнут зарабатывать нелегальными взломами, а некоторые даже получают тюремные сроки в США. Сам он в итоге от идеи зарабатывать взломами отказался, потому что не мог «воспитать в себе параноика»: «Это ведь постоянный стресс, нужно всегда быть осторожным».



У его коллег по форуму таких проблем не было, и они открыто предлагали свои услуги всем желающим. Многие из подобных сайтов существуют и сейчас — и там по-прежнему можно найти коммерческие предложения: за деньги можно купить вирус, взломать соцсети или почти любой мессенджер (кроме *Telegram*), заказать слежку за своими близкими, организовать DDoS-атаку или накрутить себе рейтинг в игре GTA5. Объявления выглядят так [21]:

Узнаем оригинальные логин и пароль ЖЕРТВА НЕ УЗНАЕТ О ВЗЛОМЕ. Удаленно взломаем любой компьютер и получим доступ к любым данным и информации на компьютере, работаем 24 часа в сутки.

Предоставляю услуги по устранению сайтов и серверов с помощью DDOS атак. Работаем с профессиональными приватными программами, которые устранят, положат, уронят, и приостановят работу сайта или сервера на заказанный вами ресурс. С нашей помощью вы устраните конкурента, или врага, который перешел вам дорогу, или помешал вам в бизнесе. У нас лучшее соотношение цены и качества на рынке ddos услуг, обращайтесь.

Как правило, хакеры обещают клиентам анонимность, скидки при длительном сотрудничестве и «индивидуальный подход». Один из людей, предлагающих такие услуги, рассказал мне, что одна из главных статей его дохода — взлом паролей по заказу. По его словам, денег такая работа приносит много, а делать ее, как правило, очень просто — большинство людей по-прежнему пользуются паролями вроде 124567 или *qwerty*.



## Глава 5

### Школа для взломщиков

Пока первые хакеры формировали собственные сообщества, на новый род занятий обратило внимание и государство. В конце 1990-х и начале 2000-х в большинстве российских технических вузов появились кафедры информационной безопасности. Самые сильные из них — в МГУ, МФТИ, университете имени Баумана, петербургских ЛЭТИ и университете информационных технологий, механики и оптики. Выпускники этих вузов к середине 2000-х стали пользоваться большим спросом на новом рынке труда: компании начали массово нанимать «пентестеров» (людей, проверяющих информационную безопасность бизнеса с помощью смоделированных кибератак).

Уже к середине 2010-х математики, программисты, специалисты по кибербезопасности захватили мир. Их влияние усиливается с каждым годом из-за постоянного роста количества средств слежения за гражданами, уязвимости личной информации, сбора больших данных — таких математиков исследователи, например, называют [\[22\]](#) создателями WMD (*weapons of math destruction*).

Впрочем, российское компьютерное образование создавалось вовсе не с нуля. Еще с 1960-х элитные советские математические школы и вузы, куда поступали их выпускники, готовили победителей международных олимпиад и будущих успешных ученых; постепенно эта система дополнилась разветвленной сетью выездных лагерей и сборов для юных математиков и компьютерщиков. Все эти институты сохранились и после распада СССР. Именно благодаря им российские подростки годами выигрывают мировые чемпионаты по программированию. Один из моих собеседников говорил, что российские хакеры стали лучшими в мире именно благодаря сильной системе образования: даже если конкретные взломщики сами не учились в матлицеях или вузах, они все равно так или иначе представляют эту школу.

«Во всей этой истории очень важна математика, — объясняет Андрей Лопатин, сотрудник петербургского университета ИТМО и тренер юных российских программистов. — Все успехи можно напрямую связывать с сильной российской матшколой. Петербургская матшкола играет в этом большую роль, особенно 239-й лицей и кружки при Аничковом дворце. Я сначала там решал задачи по информатике на бумаге. Туда же ходил и Николай Дуров». (Николай — брат основателя «ВКонтакте» и *Telegram* Павла Дурова; именно он отвечал за программирование в обоих проектах.)

В Летнюю компьютерную школу — она проводится в июле-августе в одном из санаториев под Костромой — каждый год приезжают по 200 школьников со всей страны (есть у ЛКШ смена и в зимние каникулы). Нередко поездки оплачивают региональные власти или большие российские интернет-компании — «Яндекс» или «ВКонтакте»; туда же многие выпускники ЛКШ уходят работать, окончив университет. В школе изучают алгоритмы, структуры данных, теоре-



тическую информатику. Каждый день подростки по 4 часа занимаются математикой; после обеда самостоятельно решают задачи.

«Советская и российская матшколы — это прежде всего очень сильные внеклассные занятия, — объясняет Лопатин. — На них рассказываются вещи за пределами школьной программы: они помогают быстро комбинировать идеи и для олимпиадного программирования, и для работы в корпорациях, и для чего-то другого».

То есть, например, для взломов. Российский хакер, ездивший в ЛКШ, вспоминает в разговоре со мной, что именно там научился быстро думать и изобретать оригинальные решения. Сам он до шестого класса увлекался чистой математикой, но как только у него появился постоянный доступ к компьютеру, начал увлекаться информатикой. Пока на уроках компьютерной грамотности одноклассники играли в *Need for Speed*, он изучал языки программирования и писал свои первые программы. «Поиграть я всегда мог — меня с уроков математики отпускали в компьютерный класс, потому что на самих уроках мне делать было нечего, — вспоминает мой собеседник. — Для меня все задания там были — устный счет. Учительница знала, что я пойду не в игры играть, а делать что-то толковое». Потом он начал ездить в ЛКШ, потом — поступил в МГТУ имени Баумана на факультет информационной безопасности, но не доучился и вскоре стал зарабатывать на простых взломах, получая заказы через форумы.

ЛКШ — не единственное внеклассное мероприятие для талантливых подростков-программистов. Летом 2017 года я оказался в Петрозаводске — столице Карелии на берегу Онежского озера, где каждую зиму проходит самый престижный слет такого рода: в течение недели около полусотни школьников соревнуются друг с другом, решая задачи и готовясь к международным чемпионатам по программированию. «Петрозаводские сборы — самые древние, — рассказывает один из их организаторов Андрей Станкевич. — Почему наши ребята такие крутые? В том числе из-за того, что в СССР была построена сеть матшкол — мероприятия по программированию потом делали по их образцу».

Станкевич, выигравший несколько олимпиад по информатике в юности, в середине 2000-х стал курировать сборы программистов и возглавил команду петербургского ИТМО, которая побеждала на российских соревнованиях больше других. По его словам, после нескольких побед на олимпиадах и чемпионатах молодыми программистами начало интересоваться государство. Станкевич даже участвовал во встрече с Владимиром Путиным: как он объясняет, такие мероприятия хорошо подходят для поисков дополнительного финансирования спортивного программирования. После той беседы программирование внесли [\[23\]](#) в перечень дисциплин, которые преподают в лагере для одаренных детей «Сириус» в Сочи, созданном по инициативе Путина.

В 2013 году, продолжает Станкевич, подростками-компьютерщиками «очень заинтересовались» военные из Мини-



стерства обороны. Поначалу им было непросто. «Им тяжело заинтересовать наших, потому что у них там много ограничений. По передвижению, всему прочему. А у нас тут ребята космополитичные, хотят быть мобильными, — объясняет Станкевич. — Но я знаю, что некоторые ребята, которые учились у нас в летних школах, теперь учатся в академии ФСБ».

Со временем Минобороны и связанные с ним структуры (например, Ассоциация руководителей служб информационной безопасности, которую возглавляет бывший сотрудник КГБ и ФСО Виктор Минин) начали организовывать и собственные хакерские конкурсы: на них нужно, уложившись в определенное время, взломать какую-нибудь систему. В паузах участники конкурсов слушают выступления сотрудников министерств обороны и связи — те рассказывают [\[24\]](#) о подготовке «будущих защитников информационного пространства», о структуре ЦРУ и о хакерских группировках.

Борис Мирошников, много лет возглавлявший отдел по расследованию киберпреступлений в МВД, еще в 2005 году заявлял [\[25\]](#) на конференции о киберпреступности, что «российские хакеры — лучшие в мире». «Вчерашние подростки, бессистемно промышлявшие хакерством, выросли и усовершенствовали свои методы. Раньше этим занимались озорные мальчишки. Теперь они выросли, — говорил полицейский. — Они осознали, что если ты в чем-то хорошо разбираешься, ты должен использовать это, чтобы заработать на жизнь. Они стали хакерами и объединяются через сети, чтобы разбогатеть. Всем известно, что русские сильны в математике. Наши программисты лучшие в мире, поэтому и наши хакеры лучшие в мире».



## Глава 6

### Выпускник

Большинство выпускников технических университетов не становятся хакерами в полном смысле слова. Они уходят в профильные НИИ, связанные с Минобороны (подробнее о таких учреждениях — в главе 27), или начинают работать в частных IT-компаниях, которые с середины 2000-х начали активно возникать в России. Впрочем, некоторые из них легально предлагают примерно те же услуги, которые киберпреступники продают за деньги на своих форумах. Например, слежку за людьми.

В середине 2000-х в одной из сильнейших математических школ Москвы — № 1543 на юго-западе — учился высокий и улыбчивый школьник Артем Кухаренко. До школы он добирался на междугороднем автобусе из подмосковного Троицка; дорога обычно занимала около полутора часов в одну сторону — мимо Внуково, завода «Мосрентген», через МКАД.

Кухаренко с пятого класса ходил в кружки по информатике, летом ездил в компьютерные школы, где учили алгоритмическому программированию, структурам данных, методам их анализа; в 2006 году он победил на всероссийской заочной олимпиаде по информатике. После школы Кухаренко поступил в МГУ на факультет вычислительной математики и кибернетики, даже не думая про другие варианты. На втором курсе он ходил на спецкурс «Введение в компьютерное зрение», а в конце того года после собеседования попал в лабораторию компьютерной графики и мультимедиа при факультете. В лаборатории проводились эксперименты по машинному обучению и нейронным сетям [\*\*\*]. Ближе к четвертому курсу по совету заведующего лабораторией Кухаренко обратил внимание на новую и неизученную область — распознавание лиц.

После выпуска из университета Кухаренко сменил несколько работ и часто путешествовал. В 2015 году на новогодних каникулах у него оказалось много свободного времени, и он от скуки написал приложение, определяющее породу собаки по фотографии, — для этого они с девушкой вручную разметили на 150 фотографиях собак их породы и загрузили их в самообучаемую нейронную сеть. Приложение не стало популярным, но следующей весной Кухаренко отправился с ним по возможным инвесторам. Им он рассказывал, что нейросети с распознаванием лиц — это будущее, и к 2020 году этот рынок вырастет до 6 миллиардов долларов. Некоторые поверили — так появилась компания *N-Tech. Lab*.

Один из инвесторов и кураторов проекта — Александр Кабаков. Он друг Василия Бровко, сотрудника «Ростеха», который, по словам Александра Вяри, испытывал программы для DDoS-атак на сайте slon.ru. Кабаков и Бровко вместе отдыхают и путешествуют — судя по фейсбуку, в 2016 году они делали это почти каждый месяц. Еще один инвестор — Максим Перлин, связанный с прокремлевскими молодежными движениями; его самый известный проект — эроти-



ческий календарь со студентками МГУ, выпущенный в 2010 году ко дню рождения Владимира Путина.

Весной 2015 года компания Кухаренко въехала в небольшой офис в незаметном бизнес-центре недалеко от Тишинской площади в Москве. *N-Tech. Lab* занимали целый этаж, но в офисе было пусто и почти отсутствовала мебель. На первые инвестиции компания приобрела четыре сервера за несколько миллионов рублей каждый — три поставили под столы программистов, еще один установили в отдельном охлаждаемом помещении. Показывая свои владения, Кухаренко, внешне похожий на Эдварда Сноудена, улыбался и хвастался: «*Google* для этих целей использует тысячу серверов, а у нас их всего четыре».

Они написали алгоритм, который назвали *FaceN*, — нейросеть, которая сама обучалась и находила отличительные признаки лиц для опознавания людей: величину глаз, фактуру бровей, форму губ и другие. Обучали сеть на миллионах фотографий; уже осенью 2015 года их алгоритм показал результаты лучше, чем у *Google*, — 73,3 % точных распознаваний лиц против 70,5 %. После победы на одном из программистских конкурсов компанию засыпали предложениями о продаже алгоритма, в том числе его хотела купить пограничная служба Турции, чтобы определять, кто переходит границу с Сирией. Были предложения и от российских спецслужб: московские власти решили подключить алгоритм к городской системе из более чем 100 тысяч видеокамер. «[Лица] людей, которые проходят мимо камер, [с помощью алгоритма] сверяются с загруженной в систему базой преступников или пропавших людей, — объяснял мне Кухаренко. — Если показывается высокая степень сходства, то предупреждение об этом отсылается сотруднику полиции, который находится рядом». Этот же алгоритм начали использовать для распознавания участников оппозиционных акций в Москве.

Параллельно Перлин предложил Кухаренко попытаться вывести его алгоритм на массовый рынок. Вместе они придумали *Findface* — приложение, которое позволяло бы по фотографии человека находить его аккаунт во «ВКонтакте». «Это стирает на хрен любую анонимность, — писал [\[26\]](#) Перлин, представляя приложение в своем фейсбуке. — Увидев симпатичную девушку в клубе, вы можете сфотографировать ее на телефон и моментально найти ее профиль во «ВКонтакте», узнать имя, интересы и отправить ей сообщение». Почти сразу же приложение начали использовать для другого: на анонимном форуме *2ch*, например, появился тред, в котором призывали искать «шкур, которые снимались в порно и работали проститутками». Приложение начали использовать полицейские: они поднимали старые дела, загружали в *Findface* фотографии подозреваемых, находили их во «ВКонтакте», а затем запрашивали у сети все данные пользователей.

Кухаренко все это не смущало: он считал, что безопасность важнее приватности. Я спросил его про пакет Яровой — как раз летом 2016 года Госдума приняла набор законопроектов, значительно об-



легчивший силовикам доступ к личным данным в интернете. «Мне вообще плевать, — ответил программист. — Я все обсуждаю в социальных сетях. Пусть ФСБ читает, с кем я спал, какие девушки у меня были. Деловая переписка? Ну узнают, сколько я зарабатываю и какие у меня клиенты. Я искренне считаю, что это никому не интересно. Проблема приватности преувеличена. Доступ к любому телефону получить элементарно, пусть спецслужбы меня читают».

В 2018 году система распознавания лиц, разработанная *N. Tech Lab*, начала работать в Москве. Как заявлял мэр города Сергей Собянин, уже к лету с помощью нее в метро задержали больше 10 человек, находившихся в розыске. Один из них, активист оппозиционной «Другой России», рассказывал, что у полицейских, которые его задержали, было специальное устройство, на котором была его фотография, сделанная камерой наблюдения, а также имя, дата рождения, адрес регистрации. Анкета светила красным и «пиликала»: оказалось, что в базу розыска его внес сотрудник центра по противодействию экстремизму. Мужчина спросил у полицейского, как он может исключить себя из этой базы. Полицейский ответил: «Никак».



# Часть II

## Деньги

### Глава 7

#### Планета хакеров

Пока в США шла золотая лихорадка доткомов, российские хакеры — чаще всего еще подростки — запустили свою собственную: воровство кредиток американских торговых сетей и данных банков и интернет-магазинов многим из них начало приносить миллионы долларов. Если в США человек с хорошими программистскими навыками мог и без хакинга пойти получать десятки тысяч долларов, то в бывшем СССР, где люди зачастую зарабатывали несколько сотен долларов в год, искушение было слишком велико.

Первым среди российских хакеров получил международную славу петербуржец Владимир Левин, который в середине 1990-х украл из американского банка десятки миллионов долларов. Его довольно быстро вычислили, а курьеров, которые обналичивали деньги, арестовали. Левина экстрадировали в США, где он провел 36 месяцев в тюрьме — смешной срок по сравнению с теми, что хакеры получают сейчас. Вскоре по мотивам истории Левина сняли несколько эпизодов для российских сериалов про бандитов, а сам хакер, вернувшись в Россию, исчез — уже 20 лет никто не знает, где он и чем занимается.

В индустрию взломы начали превращаться в начале 2000-х — с появлением специализированных форумов, которые постепенно эволюционировали фактически в организованные группировки. «Раньше хакерские группы организовывались скорее как клубы по интересам. Люди занимались примерно одним и тем же и просто обменивались опытом, объединяли усилия в решении каких-либо задач, — рассказывал [\[27\]](#) в те годы Андрей Споров, он же хакер *Sp0Raw*. — Сейчас же организация групп часто строится для работы по конкретным делам. Если после выполнения нескольких совместных дел группа оказывается состоявшейся, она может существовать достаточно долго и заниматься своей деятельностью безнаказанно, потому что внешние контакты по делам ограничены: все специалисты есть внутри группы. Остались и группы, построенные по старым принципам, но там „воспитываются“ новички, которые, набравшись опыта на работе из интереса, начинают задумываться о превращении своих способностей в материальные блага».

Споров говорил, что российский интернет начала 2000-х чем-то напоминает российские улицы 1990-х. «Сейчас идет первичное накопление капиталов у людей, которые, вероятно, никогда не имели бы такой возможности, работая легально, — объяснял он. — Интеллектуальная преступность гораздо неуловимее ее обыденного собрата. В дальнейшем накопленные средства будут инвестированы



во вполне обычные коммерческие проекты, некоторые из них существуют уже сейчас».

Главным сообществом киберпреступников в мире в начале 2000-х был российский форум *Carderplanet* — его еще называли «Планетой»: как объяснял мне один из хакеров, многим сайт и правда заменял реальный мир.

Начиналось все с сайта *carder.ru*, который в начале 2000 года создал человек, называвший себя *Script*. Из-за нескольких публикаций в журнале «Хакер» посещаемость вскоре выросла до 600 посетителей в день — тогда это было много. Вскоре *Script* закрыл форум и создал *Carderplanet*, но задачи двух ресурсов совпадали: там торговали украденными кредитками — «картоном», как их называли на форуме. На сайте зарегистрировались около 1000 человек. В 2001 году *Script* сам присвоил себе на форуме статус «Вора в законе»: его кумиром был Саша Белов из недавно вышедшего сериала «Бригада», вымышленный криминальный авторитет, которого играл Сергей Безруков.

Вскоре «Планета» стала основным местом общения всего русскоязычного киберандеграунда: кроме кардеров там общались спамеры, создатели троянов [\*\*\*], исследователи эксплойтов [\*\*\*], взломщики аккаунтов на *PayPal* и люди, специализировавшиеся на подделке документов. Хакеры обменивались новостями, инструкциями по взломам, объясняли друг другу, как обезопасить себя от слежки. Многим новичкам, оказавшимся на форуме, казалось, что у них появилась возможность быстро начать зарабатывать большие деньги.

Подражая мафии, участники форума называли друг друга «семьей» и строили внутреннюю иерархию по принципам клана; у *Script* было звание не только «вора в законе», но и «крестного отца». Один из руководителей форума описывал [28] эту иерархию так:

*Sgarrista* — зарегистрированный пользователь.

*Don* — член семьи.

*Capo Bastone* — друг семьи и «правая рука» Крестного отца.

*Gabellotto* — верховный судья. Глава службы безопасности.

*Consigliere* — советник семьи по различным важным вопросам.

*Capo di Capi* — мемберы, на которых возложена миссия защиты и помощи семье.

*Capo* — надежные люди, к которым присматривается администрация, либо люди, не участвующие в жизни форума.

*Giovane d'Honore* — модератор форума.

*Ripper* — кидала.

*Scum of Society* — отброс общества. Чаще всего этот статус присваивался за оскорбления в адрес модераторов или мемберов.

**Дятел** — человек, посягающий одинаковые объявления в разные разделы, задающий тупые вопросы, мешающий общению остальных мемберов.



«Хакеры взламывали защиту американских шопов и систем электронных переводов и собирали данные о кредитках их клиентов, — рассказывал [29] участник *Carderplanet*. — Все это добро передавалось кардерам, которые по своим каналам обналичивали деньги. После того как информация просочилась в прессу и журналисты рассказали миру о новом явлении, возможность быстро обогатиться привлекла толпы студентов. Большинство американских магазинов еще не имели опыта общения с кардерами, поэтому развести их не представляло большого труда даже для новичков. Падкий до хлявы, народ заказывал часто, много и все подряд».

Большинство постоянных жителей «Планеты» зарабатывали [30] около 5000 долларов в месяц; доход основателя и других ветеранов сайта мог достигать до 100 тысяч. Эти деньги вкладывали в недвижимость, на них открывали шиномонтажи, цветочные магазины.

*Script* объяснял [31], что занимается кардингом в том числе для развлечения: «У человека, идущего на риск, выделяется так называемый гормон счастья. И вот этот гормон, помноженный на количество шелестящих бумажек, и играет основную решающую роль, заставляющую человека продолжать заниматься этим не совсем честным промыслом. Заниматься этим не стыдно. Стыдно пусть будет нашему правительству, что подростки уже в столь раннем возрасте превращаются в расхитителей». При этом *Script*, видимо, уже тогда сотрудничал с украинскими спецслужбами. Участники форума вспоминали, что он упоминал о том, что «СБУ (Служба безопасности Украины, украинский аналог ФСБ. — Прим. Авт.) его любит».

В 2002 году *Carderplanet* провел в Одессе кардерскую конференцию. На нее приехали около 20 человек. Они гуляли по городу, ходили в сауну, ели в ресторанах и обсуждали организационные вопросы. Домой большинство участников конференции вернулись в полном восторге: они впервые познакомились с теми, с кем годами общались только онлайн.

Тогда же на форуме появился пользователь под именем *Воа* («Удав» по-английски). Он быстро стал звездой: его статьи про хакинг и кардинг в то же время как будто рассказывали вообще о жизни. Главным хитом стала статья про этикет: ее Удав написал после того, как на форуме начали сотнями регистрироваться подростки, прочитавшие про «Планету» в журнале «Хакер» (некоторые ветераны *Carderplanet* просили *Script* поменьше его рекламировать, но тот отвечал, что «денег в интернете хватит на всех», а «органам мы не нужны»). Новички писали личные сообщения завсегдатаям форума и просили научить их взломам. Удав решил сначала научить их культуре общения.

Он писал так:

я хочу работать в спокойной обстановке, не отвлекаясь на разную ерунду, особенно на откровенный, уникальный дебилизм. Итак: Мне очень нравится приветствие \*здравствуй\* или \*привет\*. \*Дарова\* и подобное я воспринимаю нормально, если



это исходит от тех, с кем я давно и плодотворно сотрудничаю. Всех остальных прошу воздержаться от такой фамильярности. Я не терплю обращение \*братэло\*, \*перец\*, \*кардерюга\*.

Четыре утра, Вы дома за компом или за бабой. Или перечитываете «Войну и мир» Толстого – Вам это в кайф в 4 утра. Заняты, в общем. Настойчивый звонок в дверь. Вопрос: Вы сразу распахиваете дверь нараспашку, не смотря в глазок или на монитор камеры, и с улыбкой приглашаете незнакомого бомжа зайти? Наливаете ему пива, расспрашиваете за жизнь, выслушиваете его просьбы, идиллия, в общем? Или все же спросите (хотя бы): Кто там? Спросите, видимо, для начала культурно какая это сука в 4 утра, бля, звонит в дверь, когда Вы никого, его мать, не ждете, и вам и так заебись? Ну дак какого же хера пачками идут запросы на авторизацию на Асю [ICQ] без ответа и привета. Там рамочка есть – «reason of authorization request», или что-то в этом роде. Совсем не трудно наклацать строчку, типа, я такой-то, по такому то вопросу. Скажи в глазок имя свое и чего пришел, другими словами.

Впрочем, по основному профилю форума Удав тоже кое-что понимал. «Схемы воровства из американских банков начались с Удава, — рассказывал [32] позже один из кардеров. — Этот мужик-энтузиаст устраивал целые симпозиумы в отелях — учил всех воровать с американских кредиток. На *Carderplanet* многие делились такими секретами. Русский хакер — человек не жадный, это ведь не какой-нибудь кибергопник, а интеллигент с духовными скрепами. Из России можно грабить Америку почти в открытую, продолжая традиции холодной войны и подкармливая ФСБ. В 2002 году было столько дыр в онлайн-платежах, что через них можно было выносить вагонами».

Были у Удава проекты и за пределами *Carderplanet*. Сайт его «Фабрики», *boafactory.net*, предлагал всем желающим сделать за три дня российское гражданство, получить диплом об окончании престижного вуза, визу или водительские права. Здесь подделывали практически любые документы так, чтобы их почти невозможно было отличить от настоящих. На новых загранпаспортах даже проставлялись штампы о въезде и выезде из нейтральных стран, чтобы паспорт не выглядел новым. Кроме того, *Boafactory* помогала сделать фальшивые кредитки. Говорили [33], что к услугам «конторы» прибегали тысячи людей.

К 2004 году кардинг в исполнении русскоязычных пользователей стал настолько массовым, что англоязычные медиа заговорили о «холодной кибервойне». Тем летом *Script* заявил, что уходит из *Carderplanet*, а вскоре один из администраторов форума опубликовал пост, в котором сообщил, что «Планету» «пора закрывать», поскольку она находится «под колпаком всевозможных спецслужб — как русских, так и зарубежных»:



Работники ФБР ходят в компанию AOL, как к себе домой, беря оттуда логи от *icq* и распечатку из истории. Сотрудники ФСБ предлагают деньги хостинг-компаниям за логи этого форума. Какими бы мы все умными ни были, сколько прокси мы бы ни юзали, в каком бы темном уголке земли ни располагался ВПН, через который мы ходим – все мы люди и всем нам присущ человеческий фактор. Мы прекрасно понимаем, что многие потеряют работу, многие просто не смогут больше зайти и пообщаться с единомышленниками, но, к сожалению, мы не собираемся подставлять свой зад для чьих-то заработков.

На сбор вещей и обмен контактами пользователям дали две недели. Один из участников *Carderplanet* на прощание написал стихотворение по мотивам песни рэп-группы «Многоточие»: «Щемит в душе тоска, и темный конопляный дым въедается в глаза, как будто слезы пытаюсь выжать. Я помню, как всегда, заходя сюда и видя черно-синий цвет, я заново будто рождался».

Несмотря на закрытие форума, вскоре его участников начали задерживать. Через год очередь дошла и до *Script* — им оказался 22-летний Дмитрий Голубов. В момент задержания он скрывался в доме своей бабушки в Одессе. Голубова обвинили в создании международной организованной преступной группы, которая похитила более 11 миллионов долларов. Ему грозило до 12 лет лишения свободы, но в итоге его освободили [\[34\]](#) из-под ареста еще до суда — после того как за него лично поручились двое народных депутатов. «Парня просто угробят, — заявил один из них. — А ведь он молодой талантливый человек. Такие ребята — это сливки нашей молодежи». На одном из хакерских форумов освобождение Голубова прокомментировали так: «Как по мне так он красавец! Спи...ить столько лаве и выйти сухим из воды такое не каждый может!»

Голубов так и не предстал перед судом. Вскоре он и сам стал политиком — и даже создал «Интернет-партию Украины». На последних президентских выборах его партия пыталась выставить своего кандидата — Дарта Алексеевича Вейдера, использовавшего образ злодея из «Звездных войн». В 2018 году Голубов стал биткоиновым миллионером.

Судьбы его товарищей по *Carderplanet* сложились по-разному. Кое-кто, решив, что денег уже хватит, просто перестал воровать и уехал из России. Один из таких людей рассказывал мне, что в лучшие времена получал от кардерской деятельности по 50 тысяч долларов в месяц, но, заработав на квартиры, дома и спорткары, решил успокоиться и осесть в одной из азиатских стран. Другие кардеры создавали новые площадки, следить за которыми было уже сложнее; по уровню влияния на киберподполье с *Carderplanet* можно сравнить разве что *Russian Business Network*, расцвет которой пришелся [\[35\]](#) на 2006-2007 годы. Некоторые бывшие участники *Carderplanet* продолжают заниматься тем же промыслом и сейчас — и как будто совсем не скрываются, например, создают открытые сообщества в социальных сетях, где ищут себе подручных и выклады-



вают видео о том, как снимают украденные деньги в банкоматах.

Хуже всего пришлось самым успешным соратникам *Script*. Мировые спецслужбы фактически объявили на них охоту — и начали отлавливать по одному.



## Глава 8

### Диссидент из Крыма

Кусок сала. Две банки соленых огурцов. Буханка черного хлеба. Чемодан с парой кроссовок и джинсами. Сборник рассказов Хулио Кортасара. Кассета с альбомом группы «Мышеловка».

Все это нашли и изъяли [36] при аресте у уроженца Крыма Романа Веги — он же Степаненко, он же Воа, он же Удав. Его арестовали в феврале 2003 года на Кипре. По словам [37] другого бывшего участника «Планеты», у Веги нашли еще и около 200 фотографий основателей и участников *Carderplanet*: он постоянно делал им поддельные паспорта.

Роман Вега окончил математический факультет Симферопольского госуниверситета, после чего работал специалистом по системам комплексной безопасности и связи. Увлекался альпинизмом, спелеологией, коротковолновыми радиостанциями, а также противозаконными авантюрами, о которых до сих пор известно не так много (и в основном — с его слов). Хакер якобы продавал не только документы, но и оружие. В 1993 году его арестовывали в Египте, а в 1999-м — в Майами. «ФБР пыталась состряпать дело, что якобы одна из моих тогдашних майамских компаний была намерена поставлять оружие и спецтехнику баскским боевикам в испанский Сан-Себастьян, — писал [38] Вега в своем блоге. — Кроме того, находившаяся в Кронштадте старая дизельная подлодка, которую хотели продать на металлолом, в бумагах превратилась в чуть ли не ядерную подводную лодку ВМФ России для перевозки кокаина в промышленных масштабах из Колумбии в Штаты». Далее Вега утверждал, что дело против него развалилось, «что не помешало Вашингтону навесить на меня 250 миллионов долларов и указать в обвинении, что я якобы был организатором и руководителем нескольких хакерски-кардерских международных группировок».

В кипрской тюрьме Вега просидел полтора года, после чего его экстрадировали в США, где около десяти лет перебрасывали из одного города в другой, не предъявляя обвинений, — он побывал в Сан-Франциско, Оклахоме, Атланте, Нью-Йорке и Санта-Барбаре. Приговор — 18 лет тюрьмы за массовые взломы и объединение сотен хакеров — он получил только в 2013 году, спустя десять лет после ареста.

В США Вега начал вести подробный дневник. Он пишет от руки и передает записи друзьям, которые публикуют их на сайте *romanvega.ru*; как и когда-то на *Carderplanet*, он пишет много — и довольно талантливо. Из дневников можно выяснить, что в американских тюрьмах он успел поработать плотником и столяром в мебельном цехе, а также закончил заочно техникум в Миннесоте. Час в неделю Вега проводит уроки японского; играет на ударных и два раза в неделю ходит на уроки фортепиано; учит французский и испанский; раз в несколько дней бегает босиком во внутреннем дворе и в это время считает бабочек — как-то за 21 километр пробега на-



считал их семь. В камере разрешают держать не больше пяти книг, а у него их около полутора сотен, поэтому над ним всегда висит угроза попасть в карцер. Последние несколько лет Вега пытается подготовить документы, чтобы его перевели досиживать срок в Россию, частью которой теперь является его родной Крым.

Некоторые свои заметки Вега называет «хроникой текущих событий», видимо, имея в виду диссидентский правозащитный бюллетень, выходивший в СССР с 1968 по 1984 годы. Иногда он отвечает на вопросы посетителей сайта. Например, когда его спросили, изменил ли бы он что-то в своей жизни, если б знал, что попадет на 20 лет в тюрьму, он написал, что «страшнее тюрьмы физической — тюрьма внутренняя, тюрьма души». «Что лучше: жить в полную силу, пробуя себя в том и этом, смело идя навстречу новому опыту, навстречу опасностям и приключениям, не боясь трудностей, преодолевая их на грани своих возможностей, проходя через испытания, через дела, города и страны, через победы и поражения, через горести и радости; или же, таскаясь всю жизнь на какую-то опостылевшую работу, влачить убогое существование, с единственной мыслью „как бы чего не случилось?“, как бы не рухнул жалкий мирок боящейся жить души? Что лучше? Каждому свое, — писал Вега. — Помните у О’Генри? „Дело не в дорогах, которые мы выбираем, а в том, что внутри нас заставляет выбирать наши дороги“».

В феврале 2016 года в его тюрьме появился новый заключенный по имени Михаил Горбачев. Вега заинтересовался — выяснилось, что так зовут одного из афроамериканцев: тот рассказал, что мама придумала ему имя, когда, сидя с косяком перед телевизором в 1989 году, увидела на экране советского генсека, рассказывающего про перестройку. Чернокожих, сидящих в тюрьмах, Вега вообще недолюбливает: «Если их всех таких здесь выпустить на свободу, то в стране неизбежно и быстро наступит полный и уже окончательный хаос, резня и разруха, а нормальным людям (кто выживет) придется валить со всех ног». Бывший хакер Дмитрий Насковец рассказывал [\[39\]](#), что Вега — патриот России и всегда считал США врагами, которых «надо душить».

Американская тюремная система — любимая тема Веги: он знает, что в США больше заключенных, чем в любой другой стране мира, и охотно цитирует статьи Адама Гопника из журнала The New Yorker, написанные по этому поводу. Когда в 2011 году в тюрьме Вега получил письмо от избирательного штаба Барака Обамы с просьбой поддержать его кампанию по перевыборам (это обычная фандрайзинговая практика в США), хакер ответил гневным письмом [\[40\]](#) на шести страницах — о рабском труде и несправедливости:

Соединенные Штаты Америки отобрали у меня свободу, солнце (только и видим его раз в несколько месяцев из окна тюремного автобуса по дороге на суд) <...> правосудие; отобрали и возможность видаться с матерью — ей все время отказывает в визе ваше доблестное американское посольство.



Граница на замке. 70-летняя мать ну никак не может встретиться с сыном, которого десятилетие держат без приговора. Твоя страна забрала мое здоровье и даже мои зубы.

Еще Вега часто упоминает «Архипелаг ГУЛАГ» Солженицына, особенно когда рассказывает о бездоказательных, по его мнению, процессах против американских русских. О своем хакерском прошлом человек, когда-то называвший себя Удав, в дневниках почти не вспоминает.



## Глава 9

### Белорусский Али-Баба

В 2004 году белорус Сергей Павлович, бывший завсегда́тай сайта *Carderplanet*, купил себе новый «мерседес» и повесил на него номер 999. Потом он отпраздновал день рождения *DumpsMarket* — своего кардерского сайта. Вечеринка на даче длилась четыре дня, и на нее приехали большинство хакеров СНГ. «Алкоголь лился рекой, на столах танцевали шлюхи, пацаны нюхали кокаин», — вспоминал Павлович. Гости развлекались, стреляя из пистолетов по банкам; повара вылавливали прямо из озера карпов и осетров и жарили их на гриле.

Вскоре после этого Павлович отправился в гости к подруге. Вслед за ним туда приехали полицейские.

Пока они обыскивали дом, подруга сказала ему: «Зайчик, ты слышишь меня? Слушай. Что с тобой будет — неизвестно. Сейчас ты можешь сделать только одно: поесть. Потому что когда еще в следующий раз будет такая возможность». Она положила ему плов, шашлык, в карман куртки спрятала кусок хлеба. Его увезли в полицию, а через некоторое время белорусский суд приговорил Павловича к шести годам заключения за кардинг.

В тюрьме он написал мемуары «Как я украл миллион. Исповедь раскаявшегося кардера», в которых подробно вспоминал, почему и как стал хакером. В них много печали и много поэзии. «Моя жена, скорее всего, бросит меня. Дед, который меня воспитал, умрет [к тому времени, как я выйду из тюрьмы], — писал Павлович. — Мать состарится — больше от горя, чем от возраста. Для друзей стану призраком, с которым не о чем говорить».

Павлович уверен, что стал хакером из-за бедности и проблем в семье: «Больше всего киберпреступников [на территории бывшего СССР] — от безденежья. Мозгов у людей хватает, а реализовать себя смогли только в криминале». Компьютер у Павловича появился, когда ему было всего 12 лет, — большинство его друзей тогда еще играли в приставки вроде «Денди». Несмотря на это, большую часть свободного времени мальчик проводил в компьютерных клубах: домой ему не хотелось, потому что мать устраивала пьянки с незнакомыми мужчинами. Он играл в *Counter-Strike* и *Heroes of Might and Magic 3* — и как-то раз в перерыве между битвами наткнулся на *Carderplanet*.

Оказавшись на сайте впервые, он почувствовал себя, как «Али-Баба, который наткнулся на пещеру доверху наполненную сокровищами». Подросток понял: он нашел легкий способ разбогатеть, не отходя от компьютера. Если за обычную работу он мог получить около 200 долларов в месяц, то выполнение инструкций кардеров сулило ему миллионы. Он зарегистрировался на форуме, а через некоторое время создал свой: *DumpsMarket*, рынок для перепродажи украденных кредитных карт, фальшивых документов. «Дампы» [\\*\\*\\*](#) он получал от других хакеров — или продавал то, что украл сам.



И Павлович, и другие хакеры с «Планеты» предпочитали воровать только у иностранцев. «Жалко было [атаковать цели на территории бывшего СССР], — объяснял он. — В Америке все банковские счета застрахованы, а у нас владельца карты по милициям затааскают, все будут подозревать, что он сам у себя украл, а теперь еще и вернуть хочет. На наш век и буржуев хватит. Проявление патриотизма, что ли. Холодная война продолжается, сейчас ее новый виток, только в киберпространстве». Павлович признавался [41], что «никогда не смог бы украсть кошелек в общественном транспорте», но в интернете «не чувствуешь той грани, после которой начинается преступление». Еще он говорил, что «намного проще взломать выборную систему, чем банки». Деньги Павлович хранил наличными в чемодане, который он закопал в огороде у деда.

«Я полностью посвящал себя работе, выкуривал по две пачки крепких *Marlboro*, набрал десять лишних килограммов, а специфический характер моих занятий не предполагал активного поиска новых друзей, — рассказывал Павлович. — Неудивительно, что в ту пору я спал в основном с дорогими шлюхами — высокие доходы позволяли мне иметь лучших из них. С миллионами жизнь особеннее, ярче, счастливее. Я тратил деньги иногда бездарно, иногда очень умело. Самый красивый способ расстаться с деньгами — это, конечно, женщины. Но самый приятный и, наверное, правильный — стать Санта-Клаусом, спасти жизнь тяжело больному человеку, оплатив ему операцию. Маме — новую машину, племяннику — компьютер и скутер, маме герлфренд — оплатить путешествие к океану, туда же — маму своей бывшей герлфренд». Когда Павлович однажды решил лично познакомиться с другим хакером, они заодно пригласили на встречу двух порноактрис.

Однажды у него украли со счета в *Webmoney* около 10 тысяч долларов. Когда он узнал IP-адрес вора, он заплатил знакомым сотрудникам ФСБ около 300 долларов, чтобы узнать его домашний адрес. Оказалось, что там был прописан пенсионер с 12-летним внуком. Он оставил их в покое.

Из тюрьмы Павлович вышел досрочно — в 2007 году. Почти сразу же он вернулся к кардингу, продаже оружия и созданию порносайтов, а параллельно консультировал местные спецслужбы: те подозревали заместителя начальника отдела по борьбе с киберпреступлениями в том, что он сам стал кардером. После тюрьмы начал активно заниматься спортом и сидеть на сайте знакомств «Мамба», а также думал о том, чтобы начать выпускать собственную водку под брендами *Hacker* и *Carder*, решив, что водка — «идеальный маркетинговый продукт». Проект в итоге не состоялся: «Большая часть времени проходила в погоне за женщинами».

В 2009 году Павловича вновь задержали. На этот раз суд приговорил его к 10 годам тюрьмы за воровство данных и сбыт поддельных банковских карточек. В это же время его разыскивали американские спецслужбы: Павловича считали участником группировки,



совершившей [\[42\]](#) «крупнейшее хищение в истории США» — около 100 миллионов кредитных и дебетовых карт.

Америке Павловича не выдали. «Если бы его судили там, то ему вполне могло светить пожизненное заключение. Так что ему еще повезло, что арестовали его мы, а не они», — говорил в 2009 году начальник управления «К» КГБ Белоруссии Игорь Черненко. Во второй раз Павлович вышел из тюрьмы в 2015 году и запустил сайт *Carding Pro*, на котором выкладывает инструкции о взломах и другие статьи. Среди прочего Павлович опубликовал материал [\[43\]](#) о своих бизнес-планах — он собирается производить водку под брендами «Кардер» и «Хакер».



## Глава 10

### Авантюрист с Tesla

В начале августа 2010 года Владислав Хорохорин сидел [44] с коктейлем в зале ожидания аэропорта Ниццы. Он возвращался домой после отпуска в Монако. В этот момент в помещение забежали спецназовцы в масках и с автоматами.

Полиция в разных странах искала его еще с 2003 года, когда он называл себя *BadB* и был последним из руководителей форума *Carderplanet*, остававшимся на свободе.

Родители Хорохорина развелись, когда он был ребенком; детство он провел с матерью. Денег не хватало — в том числе на хороший интернет. Тогда Хорохорин взломал систему безопасности провайдера. Когда его вычислили, владельцы провайдера обратились не в полицию, а к бандитам, как это водилось в девяностых. Подросток отделался испугом, а вскоре они с матерью переехали в Израиль. Там он пошел служить в армию — и теперь взломал ее базу данных, чтобы чаще ходить в увольнение. Его снова вычислили — и снова без серьезных последствий. В те же годы Хорохорин познакомился с основателем *Carderplanet*, хакером *Script*, — попросил у того украденную карточку, чтобы заплатить за доступ к порносайту. Вскоре они оба были одними из самых успешных кардеров мира.

Знакомый Хорохорина называл его «беспринципным и азартным». «Он был авантюристом мирового масштаба. Его любимым выражением было „Красть — так миллион. Спать — так с королевой“, — рассказывал [45] его соратник по *Carderplanet*. — У него периодически совсем не было денег, потому что он постоянно их тратил на рулетку, выпивку, шлюх».

Он любил широкие жесты. Однажды Хорохорин и Павлович отправились в ночной клуб и «сняли» там всех стриптизерш. Хакер увлекался яхтами, дорогими автомобилями — незадолго до ареста он купил себе одну из первых *Tesla*. Деньги на это были: только взломав *Royal Bank of Scotland*, они с сообщниками заработали почти 10 миллионов долларов.

После того как *Carderplanet* закрыли, Хорохорин не прекратил заниматься кардингом, а вскоре начал использовать для продвижения своего бизнеса патриотические символы и образы Владимира Путина. В 2007 году на одном из хакерских форумов он разместил рекламное объявление, в котором рассказывал, что торгует базами украденных карт уже около восьми лет. Проиллюстрировано оно было рисунком, на котором Владимир Путин вручает медали хакерам; надпись гласила: «Мы ждем вас, чтобы бороться с империализмом США. Таким образом мы инвестируем средства США в российскую экономику и способствуем ее росту».

В 2007 году Хорохорин выпустил мультфильм в двух частях [46], призывавший хакеров атаковать США. В них хакер в ушанке и тельняшке передает данные другому киберпреступнику, а тот обналичивает кредитные карты. После этого у бывшего госсекретаря США



Кондолизы Райс выпадают глаза, а Джордж Буш-младший стреляет себе в голову, поскольку из Белого дома исчезли все деньги. В конце ролика нарисованный Путин награждает хакеров медалями в Кремле.

После задержания в аэропорту Ниццы Хорохорин провел два года во французском СИЗО, ожидая экстрадиции в США. Параллельно он распродал свои активы: дом в Израиле, стоивший около миллиона долларов, виллу во Франции за 3 миллиона евро. В Америке он заключил сделку со следствием и выдал властям свою переписку с другими хакерами. Предлагали ему и дать показания против Романа Селезнева — он фигурировал на *Carderplanet* под ником *nCux*. Хорохорин утверждает, что отказался, заявив агентам ФБР: «Парни, мы в бане вместе гуляли. Какие показания? Идите на хуй».

Он получил 7 лет тюрьмы, а когда его досрочно освободили, то экстрадировали в Израиль. Российскому госканалу, приехавшему на интервью, хакер рассказал [47], что, находясь в заключении, он нашел дыры в безопасности американских военных организаций. После чего заявил, что мечтает работать на российские спецслужбы. «Русских хакеров преследуют, это охота на ведьм, они создают врага себе, — заявил Хорохорин. — Я воровал, но не у людей, а у американского государства. У них надо воровать. Они воруют у всего мира». Через пару месяцев после выхода этого сюжета хакер начал путешествовать по России.

Сейчас Хорохорин выкладывает в своем фейсбуке ностальгические фотографии, сделанные до ареста, и философские размышления о жизни. «Мне 35 лет, — пишет он. — Я феерически талантливый идиот, говорящий на 8 языках и посмотревший мир. Иногда я хочу изменить мир. Но как я могу изменить мир, если я не могу изменить себя? Недавно, на другом конце света, я встретил людей, которых не видел очень давно. У этих людей красивые и умные жены, а у одного из них двое прекрасных детей, эти люди изменились, любят и любимы, и тех людей, которых помнил я — уже не узнать. Я же не изменился ничуть. Поэтому сегодня я повторяю, как мантру: „Господи, дай мне спокойствие принять то, чего я не могу изменить, дай мне мужество изменить то, что я могу изменить. И дай мне мудрость отличить одно от другого“».

А еще, как и многие российские хакеры, Хорохорин пишет стихи:

Но кто же Вы теперь? Вы поколение Facebook и Lady Gaga,  
Где исчисляя по количеству «лайков» Оцениваете качества «френдов»  
Или сливая злость на всё и вся вокруг, ты остаешься виртуальной,  
— И рада; За «авой» лишь следы ночей без снов,  
Глаза опухшие от грустных мыслей и от слез, За «ником» комплексов покров,  
И что скрываешь ты в душе, моя отрада? Что ищешь ты — там не найдешь ответа,  
Ни помощи, ни дельного совета И уж тем более того, о чем действительно мечтаешь:  
Лишь мегабайты бреда и вопросы без ответа



## Глава 11

### Псих

Перед тем как американский суд вынес ему приговор, хакер Роман Селезнев написал от руки 11 страниц текста на английском языке. Вот [48] что он рассказал:

Я родился во Владивостоке 23 июля 1984 года. Мне было два года, когда родители развелись. Мы с мамой стали жить в комнате общей площадью 10 квадратных метров. Мы жили вместе с другими 4 семьями в эти трудные времена. Когда мне было 7 лет, моя мама купила квартиру у своего брата. Она не заплатила полную стоимость и должна была выплачивать деньги в течение года. Мы жили бедно, мне было больно смотреть, как маме приходится каждый день страдать. Она работала кассиром в одном из районных магазинов, и большую часть времени я был дома один. Так – самостоятельно – я начинал изучать компьютерные технологии. У меня появились хорошие навыки. Когда я учился в школе, понял, что надо как-то помогать матери. В 16 лет я пошел в колледж, где изучал математику и информатику. Я хотел сделать жизнь матери лучше и хотел, чтобы у меня был отец, который бы мной гордился.

Я стал замечать, что мама часто выпивает. Иногда она делала это 7 дней подряд. Когда мне было 17, мама умерла. Я вернулся из школы и увидел, что она утонула в ванной. Она умерла из-за алкогольного отравления. На следующий день брат матери забрал из квартиры все ее украшения и хорошие вещи, а мне сказал уходить. Он сказал, что мама так и не заплатила ему за квартиру, хотя она платила.

После похорон я больше не появлялся в школе. Начал искать работу. Иногда мне помогала бабушка.

Я нашел работу в местном компьютерном клубе. Они предложили работать 24 часа каждый день. Платили примерно 5 долларов за день. Скоро я понял, что они просто используют меня. Я попытался найти работу в интернете. Это привело к тому, что все пошло под откос. Я занялся криминалом. Выбрал не тот путь – стал хакером, стал взламывать компьютеры, воровать кредитные карты и другую информацию, которую можно продать. Этих денег хватало. В 2007 году я нашел большую базу кредиток и продал ее за большие деньги. Я становился жадным.

В 2008 году я женился на Светлане. В следующем году у нас родилась прекрасная Ева. Они уехали в отпуск. Я остался дома. Тогда внезапно в квартиру ворвались грабители. Они избили меня, узнали мои пароли, забрали мои компьютеры. Они знали, чем я занимаюсь, и понимали, что их не будут ловить. Я не переживал из-за материальных потерь, но снова остался без денег. Но я знал, где их достать. Я боялся, что



грабители могут вернуться, поэтому мы уехали для безопасности на Бали.

В середине 2010 года у меня были проблемы с работой, я не мог ничего найти. Поэтому снова занялся тем, что умел. В то же время у меня умерла бабушка – она была для меня настоящим родителем. Она не знала меня с плохой стороны – думала, я просто компьютерный специалист.

(Следующие несколько предложений вымараны цензурой. Очевидно, речь идет про отца Селезнева Валерия – депутата Госдумы от ЛДПР. – *Прим. Авт.* ) Он пригласил меня с семьей в Марокко. Мы приехали туда за день до того, как приедет отец. Мы решили позавтракать в отеле, но там сказали, что пустят, только если я надену пиджак. У меня пиджака не было, поэтому мы отправились в ближайшее кафе. Официант сказал, что нам придется подождать около получаса. Он добавил: «Это плохая идея». Но я не понял, что он имеет в виду.

Официант принес нам апельсиновый сок, в этот же момент шахид подорвал себя. Все кафе взорвалось [49], везде были мертвые люди и кровь. Взрывом повредило половину моей головы. Слава богу, моя жена не пострадала. (Как выяснится позже, 29 апреля 2011 года террористы оставили в кафе в Марракеше два портфеля со взрывчаткой и подорвали их с помощью мобильного телефона. Погибли 17 человек. Марокканские власти обвинили в теракте «Аль-Каиду», но организация брать на себя ответственность за взрыв отказалась. – *Прим. Авт.* )

У меня было плохое состояние, я думал, что умру прямо там. Я впал в кому. Моей жене врачи сказали, что не смогут ничего сделать для спасения моей жизни. Мне требовалась сложная операция на мозге, которую не умели делать.

Мой отец как-то смог организовать мою перевозку на самолете в Москву. Врачи сказали отцу и жене, что я скоро умру, а если произойдет чудо, я останусь «овощем на всю жизнь». Моя жена бросила меня и улетела в свой родной город – думала, я умру.

Я не был крещен. В России люди перед смертью должны креститься – иначе попадешь в ад. К больнице был приставлен священник, он быстро по просьбе моего отца крестил меня. Но чудо случилось. После двух недель я вышел из комы. Я не мог говорить и ходить, но понимал речь и мог взаимодействовать. Через 3 месяца я смог ходить, через год восстановил речь и понимание. С мая 2011 года по конец 2012 года я провел в различных больницах. У меня были операция за операцией – на мозге, на шее. В середине 2012 года мы с женой развелись. Она сказала, что оставила меня, потому что не хотела заботиться об «овоще». Она улетела в США с нашей дочерью, забрав все деньги.



В 2013 году я снова стал взламывать компьютеры и продавать кредитки. Моя жизнь была ужасной. Я ненавидел мужчину, которого видел в зеркале. Я спрашивал Бога: «Зачем ты спас меня?» Вскоре я встретил Анну, она стала моей невестой. Она ждет меня в России. Она любит меня и поддерживает уже три года. У нее есть дочь, которую я хочу удочерить.

В 2014 году я был арестован американскими властями. Когда я попал в тюрьму, у меня был плохой английский. Я был напуган, дезориентирован, не понимал и половины того, что происходит и что мне говорят люди. Мой адвокат дал мне ужасный совет бороться, потому что иначе я получу пожизненное. Сейчас мне понятно, что всем адвокатам, которые у меня были, нужна была только публичность.

Думаю, все это цена за то, что я делал всю жизнь. Я совершил много дурных поступков и беру на себя ответственность за них. Я не идеален. Теперь я отвечаю за это, как мужчина.

Я выслушал тех, кого ограбил. Мне хотелось плакать. Некоторые из них из-за меня потеряли бизнес.

Я боюсь наказания. Но понимаю, что я причинял не только финансовые проблемы. Из-за меня люди теряли ощущение безопасности – своей, своих денег, своей информации.

Я, Роман Селезнев, хочу сказать: «Я был неправ, я сожалею».

Надеюсь, что однажды выйду из тюрьмы. Я буду работать, чтобы выплатить деньги, потерянные моими жертвам. Буду работать честно. За годы в тюрьме я получил несколько образовательных дипломов, например по «ресторанному и отельному менеджменту».

До своего ареста я катился вниз по смертельно опасной дороге.

Спасибо большое.

Как указано в материалах [\[50\]](#) уголовного дела Селезнева, когда ему было 18 лет, он перешел от увлечения программированием к первым взломам. Их он совершал под именем *nCux* — «псих», если прочитать латинские буквы по-русски; этим именем он пользовался и при регистрации на кардерских форумах вроде *Carderplanet*. Поначалу он взламывал базы данных, чтобы воровать документы (имена, даты рождения, данные паспорта, номера соцобеспечения), потом стал красть номера кредитных карт и продавать базы данных другим кардерам.

Селезнев взламывал не отдельные счета, а процессинговые системы небольших предприятий в США, через которые проходили все финансовые операции этих бизнесов. Чаще других его целями становились небольшие закусочные в Вашингтоне и других городах США. В материалах уголовного дела упоминаются несколько пицце-



рий и булочных (всего около 3700 предприятий за все годы). Малый бизнес Селезнев выбирал из-за плохой защищенности: у таких предприятий не бывает своих департаментов киберзащиты, обычно они используют плохие пароли. Благодаря такому подходу к концу 2000-х Селезнев стал одним из самых успешных кардеров мира.

Спецслужбы США начали отслеживать деятельность Селезнева еще в 2005 году. В мае 2009 года агенты ФБР встретились в Москве с представителями ФСБ. Россияне представили американцам доказательства того, что за ником *nSux* скрывается житель Владивостока Роман Селезнев. Спустя месяц, в июне 2009 года, *nSux* сообщил на форуме, что уходит из бизнеса, после чего его профили на форумах были уничтожены. В США считают, что именно ФСБ передала Селезневу информацию, что им интересуются американские власти. Переписка хакера подтверждает, что он поддерживал связь с ФСБ. Одному из своих сообщников Селезнев объяснял, что у него есть защита от центра информационной безопасности ФСБ. Также он говорил, что ФСБ знает, кто он такой и чем занимается.

Мой источник, работа которого связана с кибербезопасностью, утверждает, что российских хакеров, взламывающих зарубежные системы, почти никогда не наказывают — чаще привлекают для работы на государство. Все российские хакеры знают присказку «Не работай по ru»; иными словами — нельзя, находясь в России, атаковать российские банки и компании.

Уничтожив свой прежний псевдоним, Селезнев скоро начал действовать как *Track2* и *Bulba*. Вскоре он вывел свой бизнес на новый уровень. В сентябре 2009 года он открыл интернет-магазин украденных карт. Выглядело это почти как *Amazon*: там можно было искать по категориям, выбирая между брендами карт или разными финансовыми организациями. Власти США считают, что Селезнев перепридумал кардерский рынок: раньше украденные карты появлялись на отдельных ветках форумов, теперь процесс обмена ворованными данными был оптимизирован и автоматизирован. В апреле 2011 года в магазине Селезнева появилось около миллиона новых карт. Через пару недель после этого он улетел в Марокко и чуть не погиб при взрыве. Пока россиянин лечился, его сообщники продолжали работать над проектом, но в январе 2012 года сайт закрыли.

Выйдя из больницы, Селезнев взял себе ник *2Pac*. Он создал еще один интернет-магазин и запустил сайт, на котором можно было найти базовые инструкции о том, как красть банковские данные и использовать их. В верхней части сайта висело объявление на английском: «Тут я вам объясню, Как Зарабатывать Деньги. От \$ 500 до 5 000 и даже 50 000. Помните, это нелегальный путь! Весь процесс от начала до конца». В первый месяц работы сайта в июне 2014 года его посетили 3,5 тысячи человек.

Селезнев заработал очень много. Известно [\[51\]](#), что только через один из сервисов для переводов он получил около 18 миллионов долларов. Точный размер его состояния неизвестен: хакер полу-



чал деньги через биткоины, *WebMoney* и другие электронные кошельки. Он купил два дома на Бали, часто фотографировал пачки купюр и дорогие автомобили. У него есть фотография рядом со спорткаром на фоне собора Василия Блаженного — почти такая же, как у другого арестованного российского хакера Евгения Никулина [52] (его задержали в Праге в октябре 2016 года, обвинив во взломах *LinkedIn*, *Dropbox* и других сервисов; Никулин утверждал, что от него требовали признаться в том, что он взламывал почтовый ящик Хиллари Клинтон по приказу Владимира Путина).

Понимая, что его могут отслеживать агенты ФБР, Селезнев путешествовал аккуратно. Он выбирал страны, в которых нет экстрадиции в США, и покупал билеты в последний момент, чтобы мешать спецслужбам отслеживать свои перемещения.

В июле 2014 года он отправился на Мальдивские острова, где снял виллу за 1400 долларов в день. «Я взял себе самую дорогую виллу, у меня есть собственный слуга», — написал он одному из сообщников.

Узнав, что Селезнев находится на Мальдивах, агенты ФБР попросили Госдепартамент США использовать свои связи с местными властями. После переговоров глава полиции страны согласился задержать хакера, несмотря на отсутствие договора об экстрадиции. По данным *Bloomberg*, на Мальдивы с Гавайев прилетели двое агентов ФБР. Они вместе с полицией отслеживали перемещения Селезнева. Когда тот отправился в аэропорт, откуда должен был вылететь в Москву, его задержали. Хакера посадили на частный самолет и через 12 часов привезли на Гуам, где находилась американская военная база.

По данным уголовного дела, при себе у Селезнева был ноутбук с данными о 1,7 миллиона украденных номеров кредитных карт, а также паролями к серверам, почтовым аккаунтам и финансовым переводам.

Оказавшись после Гуама в Сиэтле, Селезнев заявил, что агенты ФБР его избивали, но суд его претензии отверг. Российский МИД назвал арест россиянина похищением и «очередным недружественным шагом Вашингтона». Отец Селезнева предложил [53] ввести против Мальдив экономические санкции. Он рассказывал [54], что Романа возят на восьми бронированных автомобилях, пересаживая из одного в другой — «делают из него какого-то интернет бен Ладе-на».

Спустя месяц после ареста Селезнева на форуме *2Pac* появилось сообщение: «Извиняемся за отсутствие обновлений. Босс попал в автомобильную аварию, он в больнице».

Прокурор заявил [55], что Селезнев — самый серьезный киберпреступник из всех, кто когда-либо представал перед судом. Обвинение называло его человеком с экстраординарными компьютерными навыками, который возвращался к киберпреступлениям несколько раз, «увеличивая масштабы атак». Ущерб от его действий



оценили в 170 миллионов долларов. Прокурор даже сравнил россиянина с Тони Сопрано, главным героем сериала «Клан Сопрано».

«Его арест — редкая победа в борьбе против восточноевропейских киберпреступников, — утверждали американские прокуроры. — Многие хакеры живут в России, которая не выдает преступников в США. Если Селезнева выпустить, то, учитывая его связи с российскими правоохранительными органами, дома он будет действовать безнаказанно».

Селезнев долго отказывался сотрудничать со следствием и затягивал процесс. В уголовном деле есть расшифровка его телефонных тюремных разговоров с отцом. В них они обсуждают «вариант дяди Андрея» — затягивание рассмотрения дела, при котором Селезнев сначала заболевает, а потом перестанет общаться с адвокатами. Он сработал: рассмотрение дела удалось отсрочить на несколько месяцев.

В итоге Селезнев все-таки признал вину — и написал от руки покаянное письмо с рассказом о своей тяжелой биографии. Вердикт ему выносили в апреле 2017 года, когда история о предположительном вмешательстве российских хакеров в выборы президента США уже несколько месяцев была одной из главных тем в американских СМИ. Его приговорили [\[56\]](#) к 27 годам — самый большой срок, который когда-либо давали в США за киберпреступления. После этого хакер сменил покаянную риторику на обвинительную. «Я политический заключенный. Я орудие для правительства США, — заявил Селезнев. — Они хотят послать сигнал всему миру, используя меня в качестве пешки. Учитывая мою травму головы, сегодняшний приговор можно считать смертельным». Его отец назвал решение «приговором людоедов».

В сентябре 2017 года Роман Селезнев признал [\[57\]](#) обвинения еще по двум делам — убытки по ним составили около 52 миллионов долларов.



## Глава 12

### Стартапер

Мировые спецслужбы охотятся не только за людьми, когда-то посещавшими форум *Carderplanet*. В последние годы США задержали в разных частях мира не менее десяти российских хакеров. Некоторых из них осудили; другие ожидают приговора. Российские власти такие эпизоды обычно называет «похищениями» — и аресты россиян правда иногда их напоминают.

К 2009 году 25-летний Никита Кузьмин преуспел и в публичном бизнесе, и в подпольной хакерской деятельности. Он стал соучредителем компании *YouDo* и написал о запуске сайта колонку [58] для *gomet.ru* — в то время *YouDo* не специализировался на бытовых услугах, как сейчас, а был площадкой для заказа рекламных кампаний. Примерно в то же время Кузьмин узнал, что специалисты по компьютерной безопасности обратили внимание на совершенные им взломы: они начали исследовать вирус-троян, который Кузьмин разрабатывал последние годы и на котором зарабатывал сотни тысяч долларов.

Кузьмин — приемный сын музыканта Владимира Кузьмина. «У Никиты свой отец, я его только воспитывал, — говорил [59] певец в 2010 году. — Он стал бизнесменом. Возможно, пошел в родного отца, которого он ни разу в жизни не видел». В 2016 году певец уже отрицал [60] родство с хакером: «Это не мой сын, это ошибка».

«Сынка я нагуляла с любовником! — рассказывала [61] мать хакера Татьяна Артемьева. — Сейчас он живет в Америке, настоящий компьютерный гений, регулярно высылает мне деньги. Помню, как Володя приехал, чтобы познакомиться с отцом Никиты. Имени этого мужчины называть не буду. Кузьмин пожал ему руку, пожелал удачи, а я отдала ему ключи от съемной квартиры».

В материалах [62] уголовного дела Кузьмина указано, что он учился в двух технических вузах, где получил «продвинутые компьютерные навыки». Мой собеседник, хорошо знакомый с хакером, сказал, что Кузьмин окончил кафедру информационной безопасности Московского университета имени Баумана.

В середине нулевых Никита Кузьмин начал взламывать ICQ: он «угонял» аккаунт у владельца и требовал деньги за его возвращение. На этом хакер заработал около 20 тысяч долларов. Примерно тогда же он получил доступ к базе паролей и логинов одной из финансовых организаций. В течение нескольких лет он выводил деньги из банков по всему миру — всего около 50 тысяч долларов. Кузьмин периодически покупал разный хакерский софт для воровства денег с банковских аккаунтов в США и Австралии, но программы часто не срабатывали, и поэтому он решил сделать свою.

Он нанял программиста — и тот за десять месяцев по проекту Кузьмина написал банковского трояна, получившего имя *Gozi*. Заплатил Кузьмин за эту работу около 20 тысяч долларов.



Продвигать свою разработку он начал под ником *76 service*. Программа была не просто вирусом, а фактически B2B-софтом для преступников без хакерских способностей. Он сдавал программу в аренду другим хакерам: примерно за 2 тысячи долларов в неделю к *Gozi* можно было получить доступ и настроить ее на необходимые цели.

Программа рассылала жертвам зараженные pdf-документы. После заражения *Gozi* подгружал на компьютер вирус, который собирал всю секретную банковскую информацию, в том числе пароли и логины для входа в аккаунт. Эта информация передавалась владельцам *Gozi* — клиенты Кузьмина могли получить к ней доступ через удобный интерфейс. Позже следователи обнаружат сервер, на котором хранилось около 10 тысяч паролей к банковским аккаунтам; они принадлежали приблизительно 300 компаниям, включая NASA; всего атакам хакеров в США подверглись 40 тысяч компьютеров.

Ущерб, нанесенный хакерами, американские власти оценивают примерно в 50 миллионов долларов.

В 2010 году агенты ФБР занялись поисками авторов *Gozi*. К тому моменту они уже изучили сам троян, знали IP-адреса, с которых проводились атаки. Спецслужбы получили разрешение на перехват переписок неизвестного российского хакера. Часть из них есть в материалах уголовного дела.

«Зачем тебе *Zeus* (вирус самого разыскиваемого в мире хакера Евгения Богачева. — Прим. Авт.)? Используй мой троян. Мой намного круче», — писал хакер.

«Сколько твой будет стоить мне?» — ответил неизвестный.

«2к в месяц, все включено. И у меня есть ботсеть и удобная админка».

В других сообщениях автор *Gozi* рассказывал, что недавно подарил своей девушке фотосессию для российского *Playboy*, а по Европе ездит на кабриолете BMW 6-й серии.

Из перехваченной переписки видно, что хакер предлагал клиенту оплатить программу, переслав деньги на его счет в «Альфа-банке» — на имя Никиты Кузьмина. Помог спецслужбам и засвеченный хакером в переписках почтовый адрес [nikita@youdo.ru](mailto:nikita@youdo.ru). Американцы также изучили аккаунт Кузьмина в «Одноклассниках» и нашли там фотографии, на которых хакер стоит рядом с BMW 6-й серии — видимо, тем же автомобилем, на котором он ездил по Европе.

19 ноября 2010 года Кузьмин написал в одном из чатов: «Поеду из Таиланда и затеряюсь где-то там». Через три дня сообщил, что находится в Бангкоке. А 27 ноября он оказался в Сан-Франциско, куда поехал по делам, не думая о возможном аресте. В аэропорту Кузьмина сразу же задержали, после чего арестовали и перевезли в нью-йоркскую тюрьму.

Когда об этом стало известно другим хакерам, работавшим с *Gozi*, они запаниковали. Один из пользователей программы, разработанной Кузьминым, писал: «Всем, кто имел дело с 76-й командой,



нужно принять меры, менять контакты, на форумах вести себя аккуратно, без особой нужды не покидать родину, а то пиздец». Другой пользователь писал: «Никита много болтал про себя, все время на одной жабе [то есть аккаунте в Jabber. — Прим. Авт.] сидел, сдал партнеров...»

Первое время Кузьмину грозило до 97 лет заключения. Сторону обвинения в деле Кузьмина представлял прокурор Южного округа Нью-Йорка Прит Бхарара. Он указывал [\[63\]](#), что, сдавая вирус в прокат, «Кузьмин сделал его доступным для тех, у кого нет серьезных познаний в компьютерных науках». «В отличие от большинства [кибер] преступлений, преступление Кузьмина — распространение и использование вируса — невозможно остановить только поимкой создателя. Он продал код *Gozi* другим, и он может использоваться дальше», — объяснял прокурор.

В мае 2011 года Кузьмин подписал со следствием соглашение о сотрудничестве и начал давать показания на сообщников — после этого их арестовали в Риге и Бухаресте.

Кузьмина защищал [\[64\]](#) Алан Футерфас; он же — адвокат сына президента США, Дональда Трампа-младшего. Ранее Футерфас защищал клиентов, связанных с мафией, а с сыном Трампа начал сотрудничать после того, как стало известно о его встрече с российским адвокатом Натальей Весельницкой: та якобы предлагала [\[65\]](#) сотрудникам президентского штаба Трампа компромат на Хиллари Клинтон. Дело Кузьмина рассматривалось долго, заседания суда то и дело переносились.

В тюрьме у хакера, видимо, был доступ к интернету. В 2011 году он смог продать свою долю в *YouDo*; в 2015 году обновлял фото в фейсбуке; за два месяца до приговора оставлял комментарии на сайте *Roem*. Например, 7 марта 2016 года он участвовал в обсуждении [\[66\]](#) инициативы администрации президента о предоставлении налоговой службе информации обо всех покупках россиян за рубежом. «Сенсация прямо!» — заметил Кузьмин.

Приговор хакеру огласили [\[67\]](#) 2 мая 2016 года. Ему назначили три года заключения и штраф в 7 миллионов долларов — к тому моменту он уже провел в тюрьме пять лет. В тот же день Кузьмин вернулся в Россию. Обвинение запрашивало срок в два раза больше, однако суд учел сотрудничество Кузьмина со следствием.

Судя по фейсбуку [\[68\]](#) Кузьмина, теперь он занимается площадкой для трейдинга в интернете и много путешествует: после освобождения он уже побывал в Вене, Амстердаме, Киеве, Абу-Даби, Сочи и на плато Путорана в Якутии. Помимо этого он решил создать религию, которая объединит всех людей на земле. Разговаривать о ней со мной он отказался.



## Глава 13

### Спортсмен

22 марта 2012 года руководитель самой успешной российской киберспортивной организации тех лет *Moscow Five* Дмитрий «Смелый» Смилянец объявил [\[69\]](#), что у команды появляется «куратор» — бизнесмен и долларовый миллиардер [\[70\]](#) Сергей Матвиенко (сын Валентины Матвиенко, спикера Совета Федерации). Он рассказал, что переговоры с Матвиенко проходили параллельно с победами команды *Moscow Five* по *League of Legends* в финале чемпионата мира. На сайте *Moscow Five* появилось совместное фото Смилянца и Матвиенко: Смилянец на ней одет в синюю толстовку *Adidas*, сын Матвиенко сидит рядом с чучелом буйвола.

Судя по социальным сетям, Смилянец вообще увлекался политикой и много общался с российскими общественными деятелями. В марте 2012 года, когда проходили выборы президента России, он выложил фотографию [\[71\]](#) избирательного бюллетеня с галочкой за Владимира Путина. Фотографию он подписал: «В нем уверен! За сильного лидера!» Через некоторое время он выложил [\[72\]](#) фото с круглого стола с представителями администрации президента, на котором «обсуждались вопросы проблематики киберспорта в России». На другой фотографии был российский флаг, поверх которого была выведена цитата из гимна: «Нам силу дает наша верность отчизне».

Перед каждым соревнованием Смилянец публично обращался к Богу. «Господи, помоги нам одержать победу на *Intel Extreme Masters* в Ганновере. Бьемся за честь Москвы, за Матушку Россию!» — написал он в марте 2012 года. Тогда же он выкладывал [\[73\]](#) картину «Благословенное утро в Москве», которую, по его словам, *Moscow Five* передал художник Никас Сафронов, обычно пишущий российских политиков и знаменитостей.

В 2003 году, по данным [\[74\]](#) *Bloomberg*, Смилянец познакомился с Владимиром Дринкманом, когда они играли в *Counter-Strike* в интернете. Смилянец в этих играх часто жульничал, используя чит-коды. Вскоре они встретились. Дринкман рассказывал, что они стали друзьями — Смилянец был для него одним из людей, с которым можно выпить водки или поехать на рыбалку.

Дринкман вырос в Сыктывкаре, со школы увлекался компьютерами, самостоятельно выучил язык программирования C++ и работал системным администратором в университете. Смилянец родился в Москве, где окончил кафедру информационной безопасности Университета имени Баумана. В самоописании своего твиттера он сообщал, что его интересуют геополитика, киберспорт и информационная безопасность. Он много общался с реальными бандитами: его знакомый хакер вспоминал, что при личном знакомстве Дринкман оказался фанатом Михаила Круга, а в 2003 года его ранили выстрелом, когда он находился в автомобиле с вором в законе — тот погиб.



По данным [75] американского уголовного дела, с 2005 года приятели начали проникать в компьютерные сети финансовых компаний, платежных систем и магазинов, получая доступ к данным о кредитных картах. Смилянец отвечал в том числе за их перепродажу — карты уходили за 10-50 долларов за штуку в зависимости от страны происхождения. Они внедрились в биржу *Nasdaq*, супермаркеты *7-Eleven*, французскую сеть *Carrefour* и другие крупные компании. За следующие десять лет они, по данным обвинения, украли около 160 миллионов кредитных карт и нанесли ущерб на 300 миллионов долларов. Американским спецслужбам на Дринкмана указал хакер Альберт Гонсалес (с ним же связывали белорусского хакера Сергея Павловича); уже через Дринкмана те вышли на Смилянца. Сам Гонсалес уже отбывает двадцатилетний тюремный срок — за воровство 130 миллионов кредиток.

В июле 2013 года спецслужбы обнаружили в аккаунте Смилянца в инстаграме фотографию, на которой он в толстовке с гербом России позирует на фоне надписи «I <3 Amsterdam» в центре голландской столицы. После этого американцы обзвонили все отели неподалеку; в одном из них им сказали, что Смилянец действительно проживает в гостинице, но сейчас спит. Следующим утром детективы приехали в отель. Оказалось, что Смилянец снял два номера. В соседнем оказался Владимир Дринкман, о местоположении которого спецслужбы даже не догадывались.

В последнем посте во «ВКонтакте» перед задержанием Смилянец выложил фотографию киберспортсменов с подписью: «Достояние киберспорта России. Плохо про них могут говорить только агенты ЦРУ и МИ-6». После ареста Смилянца начали называть «крестным отцом» киберспорта, а на *sports.ru* вышла [76] колонка, в которой говорилось, что «теперь всем понятно, откуда у Смелого были деньги на содержание команд». Позже следователи сообщили, что в группировке были еще трое хакеров — двое россиян и один украинец; их поймать не удалось.

Отец Смилянца, московский адвокат Виктор Смилянец, считает [77], что вина его сына не подтверждается никакими доказательствами. По его словам, при задержании у Смилянца не было компьютера — главной потенциальной улики. «Большее недоумение вызывают суммы причиненного банкам и другим финансовым учреждениям материального вреда, фигурируют невероятные цифры, — написал Смилянец-старший. — Американцы любят рисовать астрономические цифры и тем самым списывать миллиарды долларов долгов».

Смилянец почти сразу же согласился на экстрадицию в США. Там его поместили в тюрьму в Нью-Джерси, где он начал коротать время, изучая испанский и китайский. Дринкман боролся против экстрадиции два с половиной года. Он заявил [78] *Bloomberg*, что прочитал в голландской тюрьме «Песнь льда и пламени» Джорджа Р. Р. Мартина. Интервью он дал из психиатрического отделения



тюрьмы: туда, по словам адвоката, хакер попал после того, как Голландия согласилась на его переезд в Америку.

В сентябре 2015 года и Смилянец, и Дринкман признали свою вину. Приговор им несколько раз переносили. В феврале 2018 года Дринкмана приговорили к 12 годам заключения, Смилянца — к 4 годам, которые он уже отсидел, пока шло следствие; его отпустили из зала суда.



## Глава 14

### Адвокат

Как-то вечером в 2009 году в пражской квартире, где жил с женой выходец из России Дмитрий Насковец, погас свет. Через несколько минут в дверь позвонили. Посмотрев в глазок, жена увидела мужчину в оранжевой жилетке с надписью «Электрик». «Ой, Дима, открой дверь, я в халатике!» — крикнула ему жена. Когда он открыл дверь, кроме электрика на лестничной площадке стояли агенты ФБР и чешские полицейские. Насковцу показали ордер на арест из США, заломали руки и увезли в участок.

Насковец был одним из самых успешных русскоязычных кардеров — как он вспоминал [79] позже, в этом занятии его привлекали даже не деньги, а «принадлежность к странному закрытому клубу» (зато его девушка, когда он начал богатеть, «превратилась в Пэрис Хилтон»). После задержания белорус испытал облегчение. «Наконец-то этот странный период [ожидания ареста] подошел к концу, — вспоминал он. — Когда видишь ордер, где черным по белому написано, что следующие 40 лет ты проведешь в тюрьме, это не страшно. Больно уж нереальная цифра: это же бред и сюрреализм какой-то!»

Защищал Насковца адвокат Аркадий Бух — выходец из Баку, эмигрировавший в США в начале 1990-х. Приехав в Нью-Йорк, он сразу же начал работать юристом в сообществе эмигрантов по делам о визах, нападениях, домогательствах; в 2013 году защищал Азамата Тажаякова, одного из фигурантов дела братьев Царнаевых, которые устроили теракт на Бостонском марафоне. В последние годы Бух специализируется на защите киберпреступников — например, именно он был адвокатом Владислава Хорохорина и некоторых других российских хакеров, которых судили в США.

«Остап Бендер — в бабочке, в шляпе, в белых штанах, — описывал Буха один из его подзащитных. — Имя ему сделало ФБР, потому что подсовывало клиентов с большим пафосом. ФБР ведь каждый раз хочет создать впечатление, что арестовало серьезного преступника — к радости налогоплательщиков и ради повышения по службе. Каждый раз и каждый день — крупнейший арест в истории».

Бух говорил, что российских хакеров можно называть «российскими солдатами». «Они атакуют США и не испытывают никаких моральных проблем. В России хакеры договариваются с агентами из ФСБ, они спокойны, точно знают, что их не посадят, — объяснял он. — Они много времени тратят на исследования, атаки и прочую деятельность. Они уверены в своей безнаказанности. И в крайнем случае они либо дадут денег, либо получают условный срок».

С недавних пор Бух занимается не только юридическими услугами — он создал компанию *Cybersec*, которая занимается кибербезопасностью. Его партнер в этом бизнесе — Дмитрий Насковец: хоть ему и грозило 40 лет тюрьмы, по совету адвоката хакер пошел на сделку со следствием и вышел на свободу уже в 2015 году. Сейчас с



компанией работают десятки известных хакеров, многие из них до сих пор в розыске. Сам Насковец объясняет это так: «Как бороться против русских бандитов, никто не знает, кроме самих русских бандитов».

Хакеры, за которыми охотились американцы, в основном соблюдали основное правило российских киберпреступников — «Не работать по ru», не воровать в своей стране. Некоторых, желающих рискнуть, ловит уже собственное государство.



## Глава 15

### Затаившиеся

Летом 2015 года российский Центральный банк создал *Fincert* — центр мониторинга и реагирования на компьютерные инциденты в кредитно-финансовой сфере. Через него банки обмениваются информацией о компьютерных атаках, анализируют их и получают рекомендации по защите от спецслужб. Таких атак много: Сбербанк в июне 2016-го оценил [80] потери экономики России от киберпреступности в 600 миллиардов рублей — тогда же у банка появилась дочерняя компания «Бизон», занимающаяся информационной безопасностью предприятия.

В первом докладе [81] о результатах работы *Fincert* (с октября 2015-го по март 2016 года) рассказывается о 21 целевой атаке на инфраструктуру банков; по итогам этих событий было возбуждено 12 уголовных дел. Большая часть этих атак была делом рук одной группировки, которая получила название *Lurk* в честь одноименного вируса, разработанного хакерами: с его помощью у коммерческих предприятий и банков похищали деньги.

Участников группировки полиция и специалисты по кибербезопасности искали с 2011 года. Долгое время поиски были безуспешными — к 2016-му группировка похитила у российских банков около трех миллиардов рублей, больше, чем любые другие хакеры.

Вирус *Lurk* отличался от тех, которые следователи встречали раньше. Когда программу запускали в лаборатории для теста, она ничего не делала (потому ее и называли *Lurk* — от английского «затаиться»). Позже оказалось [82], что *Lurk* устроен как модульная система: программа постепенно загружает дополнительные блоки с различным функционалом — от перехвата вводимых на клавиатуре символов, логинов и паролей до возможности записывать видеопоток с экрана зараженного компьютера.

Чтобы распространить вирус, группировка взламывала сайты, которые посещали сотрудники банков: от интернет-СМИ (например, РИА «Новости» и «Газета.ру») до бухгалтерских форумов. Хакеры использовали уязвимость в системе обмена рекламными баннерами и через них распространяли вредоносную программу. На некоторых площадках хакеры ставили ссылку на вирус ненадолго: на форуме одного из журналов для бухгалтеров она появлялась в будние дни в обеденное время на два часа, но и за это время *Lurk* находил несколько подходящих жертв.

Щелкнув на баннер, пользователь попадал на страницу с эксплойтами, после чего на атакованном компьютере начинался сбор информации — главным образом хакеров интересовала программа для дистанционного банковского обслуживания. Реквизиты в платежных поручениях банков подменялись на нужные, и несанкционированные переводы отправляли на счета компаний, связанных с группировкой. По словам Сергея Голованова из «Лаборатории Касперского», обычно в таких случаях группировки пользуются



компаниями-однодневками, «которым все равно, что переводить и обналичивать»: полученные деньги там обналичивают, раскладывают по сумкам и оставляют закладки в городских парках, где их забирают хакеры.

Члены группировки старательно скрывали свои действия: шифровали всю повседневную переписку, регистрировали домены на фальшивых пользователей. «Злоумышленники пользуются тройным VPN, „Тором“, секретными чатами, но проблема в том, что даже отлаженный механизм дает сбой, — объясняет Голованов. — То VPN отвалится, то секретный чат оказывается не таким секретным, то один вместо того, чтобы позвонить через *Telegram*, позвонил просто с телефона. Это человеческий фактор. И когда у тебя копится годами база данных, нужно искать такие случайности. После этого правоохранители могут обращаться к провайдерам, чтобы узнать, кто ходил на такой-то IP-адрес и в какое время. И тогда выстраивается дело».

Задержание хакеров из *Lurk* выглядело [83] как боевик. Сотрудники МЧС срезали замки в загородных домах и квартирах хакеров в разных частях Екатеринбурга, после чего сотрудники ФСБ с криками врывались внутрь, хватали хакеров и бросали на пол, обыскивали помещения. После этого подозреваемых посадили в автобус, привезли в аэропорт, провели по взлетно-посадочной полосе и завели в грузовой самолет, который вылетел в Москву.

В гаражах, принадлежащих хакерам, нашли автомобили — дорогие модели *Audi*, «кадиллаков», «мерседесов». Также обнаружили часы, инкрустированные 272 бриллиантами. Изъяли [84] украшения на 12 миллионов рублей и оружие. Всего полицейские провели около 80 обысков в 15 регионах и задержали около 50 человек.

Арестованы были, в частности, все технические специалисты группировки. Руслан Стоянов, сотрудник «Лаборатории Касперского», занимавшийся расследованием преступлений *Lurk* вместе со спецслужбами, рассказывал, что многих из них руководство искало на обычных сайтах по подбору персонала для удаленной работы. О том, что работа будет нелегальной, в объявлениях ничего не говорилось, а зарплату в *Lurk* предлагали выше рыночной, причем работать можно было из дома. «Каждое утро, кроме выходных, в разных частях России и Украины отдельные личности садились за компьютеры и начинали работать, — описывал Стоянов. — Программисты докручивали функции очередной версии [вируса], тестировщики ее проверяли, потом ответственный за ботнет загружал все на командный сервер, после чего происходило автоматическое обновление на компьютерах-ботах».

Рассмотрение дела группировки в суде началось еще осенью 2017 года и продолжалось в начале 2019 года — из-за объема дела, в котором около шестисот томов. Адвокат хакеров, скрывающий свое имя, заявлял [85], что никто из подозреваемых не пойдет на сделку со следствием, но некоторые признали часть обвинений. «Наши клиенты действительно выполняли работы по разработке



различных частей вируса *Lurk*, но многие просто не были осведомлены о том, что это троянская программа, — объяснял [\[86\]](#) он. — Кто-то делал часть алгоритмов, которые могли с успехом работать и в поисковых системах». Дело одного из хакеров группировки вывели в отдельное производство, и он получил 5 лет, в том числе за взлом сети аэропорта Екатеринбурга.

В последние десятилетия в России спецслужбам удалось разгромить большинство крупных хакерских группировок, которые нарушили главное правило — «Не работать по ru»: *Carberp* (похитили около полутора миллиардов рублей со счетов российских банков), *Anunak* (похитили более миллиарда рублей со счетов российских банков), *Raunch* (создавали платформы для атак, через которые проходили до половины заражений по всему миру) и так далее. Доходы таких группировок сопоставимы с заработками торговцев оружием, а состоят в них десятки людей помимо самих хакеров — охранники, водители, обнальщики, владельцы сайтов, на которых появляются новые эксплойты, и так далее.



## Глава 16

### СЫЩИКИ

Расследованием киберпреступлений занимаются, в частности, в специальном подразделении МВД — оно называется управление «К» [\*\*\*]. Для группировок вроде *Lurk* там написали собственную аналитическую программу, выявляющую связи, которые могли упустить следователи, если загрузить в нее собранную информацию: засвеченные IP-адреса, данные серверов, сведения о хакерах, которые ранее проходили по похожим делам.

Полицейские из управления «К» работают в неприметной усадьбе Кирьякова на Петровке, напротив Высоко-Петровского монастыря и в двух минутах от клуба, где часто проходят гей-вечеринки. Заехали они в здание (которое ранее принадлежало поочередно коллекционеру антиквариата, князю Михаилу Оболенскому, ученому-терапевту и зубоврачебной школе) в конце 1990-х, когда было принято решение создать при МВД специальное подразделение по борьбе с киберпреступлениями. «Тогда пошли кардеры, и уже тогда было понятно, что одним из наших основных направлений станет противодействие распространению детской порнографии», — рассказывает мне заместитель начальника управления Александр Вураско.

Эти люди редко ходят на работу в полицейской форме — чаще в джинсах и незаправленных рубашках; у некоторых на руках *Apple Watch*. Посетителям на входе выписывают ручкой бумажный пропуск; в коридоре на втором этаже стоит застекленный шкаф с подарками, среди них фарфоровая ваза, расписанная под гжель, дар от Службы внешней разведки. Рядом лежит связка баранок.

Работающие в усадьбе занимаются самыми сложными киберпреступлениями, то есть расследуют дела хакеров, объединившихся в группы и хорошо скрывающихся. В управлении несколько десятков сотрудников, для поступления в отдел от них требуют навыков «оперативника, юриста и айтишника одновременно». Находить таких людей сложно, некоторые приходят из Московского университета МВД или Университета имени Баумана, но неизбежно переучиваются.

Каждое утро полицейские собираются в своих отделах на быстрые совещания, каждую пятницу руководство собирает все управление. У многих сотрудников работа часто начинается около пяти утра: в это время принято ездить на задержания. Там, впрочем, бывают не все: технические сотрудники в специальной «чистой» комнате без интернета исследуют изъятые носители информации и другую технику.

«Это в 1999 году можно было именоваться программистом по всему, — рассказывает Вураско. — Сейчас все крайне узкоспециализированно. Бывают ситуации, когда мы не можем самостоятельно разобраться, и не имеет смысла держать штат специалистов, которые декомпилируют вредоносные программы, когда можно обратиться к тем, для кого это хлеб, вроде *Group-IB*, „Лаборатории Каспер-



ского”, *Positive Technologies*. Они могут активно пиариться [на расследованиях], но только мы или ФСБ можем поставить окончательную точку — привлечь к ответственности».

«Наша доблестная милиция не разбиралась тогда в компьютерах, — вспоминал один из хакеров начала 2000-х. — Отдел «Р» (Будущий отдел «К». — *Прим. Авт.*) через полгода скатился к банальной прослушке за деньги. Крупную рыбу никогда не ловили и не поймают, так как крупной рыбе в России делать тогда было нечего. Банковская система в США и Европе на 50 лет старше нашей, и вариантов для телодвижений там, конечно, больше. Чаще всего люди попадались на случайностях, вещах, не имеющих ничего общего с кардингом».

По словам Вураско, многие российские полицейские до сих пор не разбираются в основах компьютерной безопасности: не знают, что такое IP, не понимают, куда отправлять запросы для получения информации по оперативно-разыскной деятельности. Управление «К» часто проводит для следователей и судей курсы, чтобы они понимали, о чем идет речь в делах, связанных с киберпреступлениями.

Управление «К» в последние годы расследовало несколько дел, похожих на *Lurk*. Работа по ним идет долго: полицейские всегда стараются выявлять всех членов группировки и заводить на них дело как на организованную преступную группировку — иначе, как показывает практика, хакеры получают условные сроки.

— Для общения между собой члены группировок обычно используют jabber-серверы и все основные мессенджеры. Организаторы все ключевые моменты обсуждали по защищенным каналам, — рассказывает Вураско о деталях дела *Lurk*.

— То есть к ним у вас в итоге не было доступа?

В ответ майор смеется и говорит: «Позвольте мне не отвечать на этот вопрос».

Полицейские из отдела «К» занимаются расследованием только избранных киберпреступлений. Они никогда не расследовали хакерские атаки на российских оппозиционеров и негосударственные СМИ, даже когда им представляли доказательства; к ним крайне сложно обратиться с заявлением о взломе почты или DDoS-атаке на бизнес — такое заявление, скорее всего, не примут.

«В виртуальном пространстве собирать улики и правда гораздо сложнее, чем в физическом, — объяснял [\[87\]](#) Алексей Лукацкий, работающий консультантом по информационной безопасности в *Cisco Systems*. — Информация собирается по крупицам и требует очень серьезных ресурсов, поэтому атрибуцией злоумышленников занимается мало кто. Если мы говорим о компьютерных преступлениях, которые происходят внутри страны, — например, когда хакерская группировка осуществляет проникновение в банк, — то эти преступления очень плохо расследуются. Ни законодательство, ни квалификация большинства следователей не позволяют эффективно проводить расследование. Все процедуры очень бюрократизированы, по-



этому к моменту, когда выдаются ордера на сбор доказательств с видеокамер, логов провайдеров связи и так далее, следы оказываются уже затерты». По словам Лукацкого, действительно хорошо дела такого рода расследуются, «если на стороне жертвы есть компания, которая может собрать и представить доказательства вместо правоохранительных органов», — но и в таком случае суд часто дает преступникам условные сроки, и они продолжают заниматься тем же, чем занимались. Дела чаще всего заводятся по статье 272 УК РФ «Неправомерный доступ к компьютерной информации».

При этом большими группировками вроде *Lurk* современная российская интернет-преступность, конечно, не ограничивается. Есть у нее и другой огромный сегмент — он находится в даркнете, части интернета, скрытой от лишних глаз. У этого сегмента тоже есть свои главные герои: как и когда-то в случае *Carderplanet*, ими тоже зачастую оказываются создатели и администраторы форумов.



## Глава 17

### Черный рынок

Автомобиль остановился на обочине рядом с лесом недалеко от МКАД. Из него вышел мужчина со свертком. Он оглянулся, подошел к нужному дорожному знаку, положил сверток с пистолетом и патронами на землю и набросал сверху листьев. Через несколько часов покупатель, знавший про ориентир, забрал «закладку».

Для «закладчика» это уже был обычный ритуал: последние годы он вел двойную жизнь. Семья, друзья, коллеги по работе знали его как любителя дачного отдыха. Он никогда не рассказывал им о том, что уже несколько лет арендует в центре Москвы звукоизолированную мастерскую, где собирает огнестрельное оружие для продажи через подпольные форумы.

Он попал в русскоязычный даркнет около пяти лет назад. Его интересовало все, что нельзя найти в обычном интернете: изготовление печатей, паспортов, наркотиков, оружия. Он зарегистрировался на *Runion*, одном из крупнейших форумов даркнета в России, под ником *Korabas*. Зайти на форум можно было через *Tor* — шифровальную программу, которая, как гарри-поттеровская мантия-невидимка, скрывает пользователя и позволяет заходить на сайты, не индексирующиеся обычными поисковиками. Технологию, на которой работает *Tor*, создали в лаборатории американского флота в середине 1990-х для защиты американских госучреждений в сети; впоследствии она была рассекречена и передана независимым разработчикам. Сейчас программа — один из самых эффективных способов обходить цензуру в интернете и сохранять анонимность. В 2013-м именно с помощью *Tor* Эдвард Сноуден передавал часть документов американского Агентства национальной безопасности журналистам.

Изучив форумы, *Korabas* собрал себе по найденным инструкциям пистолет. На производство ушло больше денег, чем он рассчитывал, но, когда он выставил оружие на продажу, его внезапно купили очень быстро, и *Korabas* решил не останавливаться и попробовать подзаработать.

Пользователь анонимно арендовал мастерскую, купил несколько станков и дрели. Помещение не отапливается, поэтому комфортно работать получается только весной и летом, но если есть заказы, приходится сидеть и в холоде. Рассказывая свою историю, *Korabas* часто использует аббревиатуру «емнип» («если мне не изменяет память»); наше общение проходит в зашифрованном чате: показывать лицо или называть свое настоящее имя чужакам люди вроде *Korabas* совсем не хотят. Разговор наш продолжается несколько дней подряд, иногда в чат добавляются новые участники, которые рассказывают подробности о некоторых операциях в даркнете.

Бизнес быстро развивался — вскоре *Korabas* нашел продавцов патронов и начал делать глушители. Со временем он стал одним из основных торговцев оружием на *Runion*. Пока другие занимались пе-



репродажей, *Korabas* покупал сигнальные пистолеты и переделывал их под патроны 9×18 миллиметров — одни из самых распространенных в СНГ. После переделки очередного пистолета *Korabas* обычно надевает на него глушитель и отстреливает прямо в мастерской в центре города: «Лень возить каждый пистолет в лесополосу на испытания». «В кино пистолеты с глушителем стреляют беззвучно, в реальности же в лучшем случае глушится 50 % [шума]», — рассказывает он.

Продажа оружия в *Tor* для него — хобби: цены в «магазине» начинаются от 60 тысяч рублей, выходит по одной-две сделки в месяц, так что годовая прибыль получается в районе 500 тысяч. «На квартиру точно не заработаешь», — пишет *Korabas* и ставит три закрывающие скобки: смеется. Хобби, впрочем, любимое: продавец и сам периодически выезжает пострелять за город. «На стрельбу не беру деньги из семейного бюджета, трачу только то, что заработал в *Tor*».

*Korabas* понимает, что его в любой момент могут задержать, а потом посадить на много лет, и ведет себя крайне осторожно. Его компьютер работает на *Linux*, жесткие диски зашифрованы, в сеть он выходит через *Tor*, заработанные деньги снимает с пластиковых карт за границей — эти карты выпущены на людей, которых сам *Korabas* не знает.

Похожей жизнью в русскоязычном даркнете живут тысячи людей. Только на *Runion* ежедневно заходят две-три тысячи человек. Администраторы и продавцы в *Tor*, которые часто занимаются деятельностью, попадающей под уголовное законодательство, крайне редко общаются с журналистами: они считают, что любой неосторожный контакт может привести к аресту.

\*\*\*

Через форумы вроде *Runion* можно не только купить оружие, но и заказать взлом или сделать себе поддельную личность. Максим ищет себе заказы именно на таких форумах и чаще всего работает через «гаранта» — специального посредника, который замораживает оплату до выполнения заказа и решает спорные вопросы, если они возникают. В основном Максим занимается фишингом [\*\*\*]; иногда на взлом требуются месяцы: большая часть времени уходит на то, чтобы собрать как можно больше личных данных о жертве. Максим взламывал российских оппозиционеров и уверен, что не раз работал на спецслужбы, хотя они никогда и не говорят о том, что они оттуда.

Максим решил работать в даркнете, после того как его знакомого чуть не посадили за взлом. Таким же путем пришел к своему нынешнему занятию другой хакер — он называет себя *Sleepwalker*.

Когда его приятель чуть не погорел, не позаботившись об анонимности, *Sleepwalker* начал создавать цифровые «личности» (или «идентичности»), со временем — продавать их. Кроме того, в русскоязычном *Tor* он известен как хакер, который за биткоины тестирует



сайты на возможность взлома и проводит консультации по анонимности.

*Sleepwalker* с детства смотрел фильмы о хакерах. «Сидит некий человек, взламывает что-нибудь, на мониторе черный фон, зеленые буквы мелькают, это казалось таинственным», — вспоминает он. На *Runion* он написал статью «Быть хакером?!», в которой вывел правило: «Хакеры испытывают удовольствие от решения проблем, от нахождения обходного пути, от понимания сути процесса». Там же *Sleepwalker* учил желающих «собирать доказательства с компьютера подозреваемого» и взламывать страницы во «ВКонтакте» — при этом мне он сказал, что не занимается взломами сайтов и аккаунтов в социальных сетях за деньги. В 2014 году *Sleepwalker* даже демонстративно украл почту и аккаунт «ВКонтакте» у школьника, который спросил, сколько будут стоить услуги по взлому.

Несколько лет назад *Sleepwalker* получил доступ к базе сканов паспортов и других документов. Он добыл ее случайно, когда перебирал пароли на сервере одного из магазинов. После этого хакер начал «специально извлекать» сканы документов у различных компаний и создавать под них «личности» в интернете.

Работу над каждой «личностью» он начинает с того, что придумывает человеку историю. После — начинает ими «жить». Для «личности под ключ» хакер регистрирует несколько аккаунтов в социальных сетях с фотографиями и 200-300 друзьями; заполняет их «продуманными интересами и мелкими деталями»; пишет на страницах посты на темы, подходящие «личности», и моделирует ее язык; регистрирует на «личность» кошельки в «Яндексе» и Qiwi; регистрирует на нее номер телефона; в редких случаях получает доступ к интернет-форумам, чтобы оставить там комментарии «личности».

Работа над «личностью» занимает около месяца. За несколько лет *Sleepwalker* продал около сотни личностей, получив за каждую 50-100 долларов.

«В создании достаточно учесть основные факторы, по которым люди в сети считают, что личность настоящая, и тогда можно стать кем угодно для провайдера, обычных людей, правоохранительных органов, — рассказывает хакер. — Это может пригодиться для различных дел вроде шантажа, позволит не только создать впечатление определенной личности, но и действительно быть ей в рамках виртуального пространства. Например, принимать и отправлять деньги, общаться от лица виртуала».

*Sleepwalker* говорит, что сложнее всего в этой работе обладать знаниями «личности», которую создаешь, то есть писать правильным языком и оставлять неглупые комментарии. «Иногда аккаунт получается живее, чем иные аккаунты обычных юзеров сети, — говорит он. — Как-то меня попросили создать умную, красивую девушку для привлечения иностранцев в фейсбук и их развода на деньги. Они полились рекой».

В разное время *Sleepwalker* создал «личности» студента, ищущего приключения, девушки, интересующейся даркнетом, копирайтера.



А для себя — старика-рыбака. Под него он подобрал сканы паспорта, зарегистрировал виртуальные карты в «Яндекс-кошельке», *Qiwi*, профиль на *Avito*. Страницу во «ВКонтакте» заполнил не до конца: «человек старый, так что так и надо».

В обычном интернете *Sleepwalker* чувствует себя неуютно: «Возникает ощущение подконтрольности чему-то или кому-то».

\*\*\*

18 июня 2016 года со мной связался представитель *Runion*, крупнейшего русскоязычного форума в даркнете. Он предложил взять интервью у «одного из самых уважаемых и влиятельных людей русскоязычного сегмента». Им оказался *Nikkon* — человек из администрации форума, в работу которого входит гарантирование сделок: он следит за тем, чтобы продавали то, что заявляют, и по условленной процедуре. В эти же дни Госдума начала рассматривать «пакет Яровой» — группу «антитеррористических» поправок, которые в том числе наносят удар по приватности в интернете. Намерение поговорить представитель *Runion* объяснил в том числе своим желанием донести до аудитории: *Tor* безопасен для общения, и там собираются не столько педофилы и продавцы наркотиков, сколько люди, которые ценят свободу распространения любой информации.

За два года до этого, осенью 2014 года, *Nikkon* сидел вечером в номере московского отеля, пил вино и читал свой форум. Закончив дела раньше, чем планировал, он ожидал самолета, который вылетал только через день. Во время командировки он часто думал о подарке для своей девушки — «хотелось чего-то небанального».

Один из знакомых по *Runion* обратился к нему с неожиданным предложением — помочь с продажей партии изумрудов.

Как официальный гарант форума, *Nikkon* периодически проводил сделки по продаже наркотиков и оружия: проверял товар и получал процент, зарабатывая от трех с половиной тысяч долларов в месяц. Впрочем, работой это администратор *Runion* все равно не считает. «Доходы от этой деятельности и основная зарплата, увы, несравнимы, — говорит он. — Может быть, учитывая темпы роста рынка, через пару лет [ситуация изменится]».

*Nikkon* ответил знакомому, что согласен на сделку. В его задачи входило принять деньги покупателя, подтвердить их наличие и дожидаться от продавца отмашки о передаче товара; качество самих изумрудов проверил другой человек.

Заканчивая сделку, он решил купить немного драгоценностей для подруги. *Nikkon* впервые оказался в «шкуре клиента»: как и любой человек, поднимающий «закладку», он волновался, что может случайно нарваться на полицейский патруль: за незаконную торговлю драгоценностями в России можно получить до 5 лет тюрьмы. Обошлось, но после этого он старался не покупать ничего в даркнете.



К тому моменту *Nikkon* провел на *Runion* около года. Туда он перешел с форумов кардеров — тех, что появились после закрытия *Carderplanet*.

*Nikkon* утверждает, что сам не занимался кардингом, а «только читал и интересовался». В *Tor* он оказался из-за «тяги к знаниям, недоступным в открытых источниках». В тот момент, по его воспоминаниям, *Tor* представлял собой «хрестоматийное собрание предрассудков, тянувшихся за ним до сих пор»: детское порно, пугающие загадочные страницы вроде игр-лабиринтов со звуковым сопровождением из детского плача. Из-за подобных сайтов подпольный интернет быстро вошел в подростковую мифологию русскоязычных нетсталкеров (исследователей интернета) как место, где на «особых уровнях» можно найти истину. На «Ютьюбе» можно найти ролики [88] о последнем уровне «глубокого интернета» — «тихом доме», где якобы хранится [89] информация «о боге / смерти / жизни и все, что только захотите».

Изучая сетевое подполье, *Nikkon* наткнулся на англоязычный форум со статьями о шифровании и наркотиках. Он воспринял их как неожиданное «богатство» — из-за «неклассической» тематики. Потом нашлись и другие форумы — многие из них, впрочем, быстро прекращали свое существование. *Nikkon* помнит, например, падение *Freedom Hosting*: в 2013 году владельца серверов, где размещались десятки *Tor*-сайтов, арестовали и назвали [90] «крупнейшим посредником для распространения детской порнографии на планете». Собеседник назвал закрытие проекта «первым серьезным ударом по *Tor*». ФБР после заявляло [91], что контролировало серверы еще до ареста владельца.

Уязвимость *Freedom Hosting* напугала многих и в русскоязычной части *Tor*; впрочем, ущерб ограничился несколькими рухнувшими сайтами. Основные площадки — ими стали четыре сайта: *Runion*, *RAMP*, *R2D2* и *Amberoad* — продолжали работать. Их создатели ориентировались на своих англоязычных коллег и в первую очередь на сайт *Silk Road*, вокруг которого к тому времени уже сформировался своего рода культ.

\*\*\*

В конце 2010 года молодой американский либертарианец Росс Ульбрихт, работавший в книжном магазине, записал в своем дневнике новую идею: «Создать сайт, где люди могли бы купить анонимно что угодно, не оставляя следов, по которым их можно было бы выследить». Несколько месяцев спустя он запустил *Silk Road* — цифровую ярмарку всего на свете; первым проданным товаром стали выращенные самим Ульбрихтом псилоцибиновые грибы. Вскоре подтянулись и другие торговцы. *Silk Road* первым объединил *Tor* и биткоины; пользоваться им вообще было достаточно просто: например, товары зачастую рассылались по почте в коробках от DVD. Именно бла-



годаря *Silk Road* тысячи пользователей «обычного интернета» узнали и о *Tor*, и о сетевой анонимности.

Узнали о *Silk Road* и спецслужбы, которые в январе 2012-го организовали специальную группу, искавшую создателей сайта. К тому моменту сам Ульбрихт зарабатывал по 25 тысяч долларов комиссионных в месяц за покупки через портал и фигурировал на *Silk Road* под именем Ужасный пират Робертс (*Dread Pirate Roberts*) — площадку он использовал не только для заработка, но и для публикации либертарианских проповедей: «Я создал новый тип экономики, чтобы люди почувствовали, как это — жить в мире без влияния власти». Он был уверен, что каждая сделка на его площадке — шаг к всеобщей свободе.

В итоге американские спецслужбы раскрыли Ульбрихта и задержали его в библиотеке Сан-Франциско. В мае 2015 года его приговорили к пожизненному заключению. Перед вынесением приговора Ульбрихт написал судье письмо: «Суть *Silk Road* должна была сводиться к тому, чтобы дать людям свободу принимать самостоятельные решения. <...> На деле это обернулось удобным средством удовлетворения человеческого пристрастия к наркотикам. Я понял, что, давая людям свободу, никогда не знаешь, что они сделают с ней».

Своими идеями Ульбрихт вдохновил многих для создания в 2012 году манифеста российского киберподполья, который часто стали использовать на форумах в даркнете: «Интернет стал опасен для человека, у нас хотят отобрать право обмениваться информацией, он становится подконтрольным, свободу слова ограничивают, людей, распространяющих свои идеи, преследуют, камерами хотят контролировать каждый шаг». Помимо этого, авторы манифеста указывали, что они люди «с обостренным чувством справедливости», продажа оружия на форуме объясняется тем, что «мы хотим сами решать, как и чем обезопасить себя и своих близких», продажа наркотиков — «Мы сами хотим контролировать то, что попадает в наш организм».



## Глава 18

### Главный спамер России

1 апреля 2013 года на форуме «Античат» появился пост одного из самых известных российских хакеров — он действовал под ником Severa:

Меня зовут Петр Севера, многие меня знают по сервису рассылок по электронной почте [\[92\]](#), который я предоставляю уже почти 15 лет. Но все течет, все меняется, и пришло время и мне сменить направление работы. Несколько дней назад я получил предложение от ЦИБ ФСБ РФ возглавить новый Отдельный Специальный Батальон Информационной Безопасности (ОСБИБ).

Это новое подразделение, которое создается для оказания противодействия кибервойскам США, Китая, Германии и других стран. В задачу ОСБИБ будет входить как оперативное устранение информационных и электронных угроз важнейшим инфраструктурным объектам Российской Федерации, так и адекватные и оперативные ответные действия на возникающие угрозы.

Мне поручено не только возглавить, но и создать основной состав ОСБИБ. Естественно, все предложенные мной кандидатуры будут обсуждаться руководством управления К и ЦИБ ФСБ, но мне дали понять, что у меня есть почти полный карт-бланш на первоначальный состав. Полная численность ОСБИБ через год будет порядка 500 человек, пока мне поручено набрать первую сотню. Для нас не важно, чем вы занимались до этого, важно то, что вы умеете и знаете, а также желание защищать свою Родину и своих близких от реальных угроз 21 века.

Требования к кандидатам:

- гражданство РФ– возраст от 18 до 45 лет– глубокие и всесторонние знания в области информационной безопасности и в смежных областях– умение быстро находить неординарные решения– умение работать в команде

Наличие высшего технического образования является плюсом, но не будет обязательным, гораздо важнее то, что вы реально умеете. Наличие законченной военной кафедры или пройденной срочной службы в Вооруженных Силах РФ также является плюсом.

Все те, кто будет отобран мной, получают после испытательного срока весь набор благ офицеров ФСБ РФ, а в дальнейшем и реальные офицерские звания. Место работы – Москва, Сколково, сейчас строится отдельное режимное здание для сотрудников ОСБИБ. Проживание для вас и вашей семьи за счет работодателя в отдельном коттедже, в благоустроенном поселке, ЗП – обсуждается индивидуально, от 150 т.р. и выше.



Я уже начал формировать списки на первичное собеседование, присылайте резюме мне в жабу jabber@honeste.com. Если вы участвовали в разработке чего-то нелегального, типа ботнетов, взлома сайтов и тп, прикладывайте к резюме отдельную пояснительную записку, дальше меня она не пойдет – хотя всем соискателям и обещана полная амнистия, гарантировать что не будут преследовать тех, кого я не выберу, я не могу. Так что лучше подстраховаться, в официальном резюме указывайте только законную информацию.

Родина вырастила нас, дала нам всем образование, теперь пришло и наше время послужить России.

Другие участники форума быстро начали отвечать: «Привет хачу в батальон что надо делать?», «Ржака. Приходите, хакиры — всех помилуем и косточку дадим, будете работать на хозяина». Были и те, кто воспринял первоапрельскую шутку серьезнее: в конце концов, Severa был одним из немногих российских киберпреступников, начавших в 1990-х, кто к тому времени оставался на свободе.

Петр Левашов, впоследствии взявший себе ник Severa, родился в Ленинграде в августе 1980 года и окончил физико-математическую гимназию, продолжавшую традиции советских матшкол (см. главу 5). В школе он увлекся и хакингом — и вскоре стал известен как создатель сетей ботов, использовавшихся для спамерских рассылок, и автор поддельных антивирусов: «проверив» компьютер, они выдавали пользователю сообщение о найденных проблемах и требовали денег за «лечение». Левашов-Severa был модератором спам-разделов на подпольных русских хакерских форумах; часто связывал хакеров между собой, знакомил новичков с основами профессии, помогал настраивать бот-сети.

Как рассказывает один из моих собеседников, знакомый с деятельностью Левашова, с середины 2000-х Severa внезапно стал предлагать другим участникам форумов помогать государству в интернете — атаковать сначала сайты чеченских террористов, а потом российскую оппозицию. Об этом же писали [\[93\]](#) журналисты Андрей Солдатов и Ирина Бороган. При этом чеченские террористы рассказывали, что им пришло письмо от «хакера Самуэля из ФСБ», в котором он предлагал остановить атаки при выполнении условий: «Цена вопроса 100 000 долларов. Можно договориться. Бен Ладен не обеднеет». Левашов призывал хакеров атаковать и хостинг-провайдеров в Швеции и Литве, где предоставляли место для сайта «Кавказ-Центра». В те же годы, по словам нескольких моих собеседников-хакеров, Левашов начал сдавать свои бот-сети в аренду прокремлевским молодежным движениям.

Зимой 2012 года ботнет Левашова включился в российскую предвыборную кампанию: он рассылал [\[94\]](#) письма, рассказывающие о гомосексуальности кандидата в президенты Михаила Прохорова. В гомофобной стране это означало черный пиар; в письмах



размещались ссылки на материал с якобы цитатой из Прохорова: «Всем знающим меня давно понятно, что я — педик».

Другие хакеры не раз подозревали Severa в том, что он сотрудничает со спецслужбами и, например, помогал им ловить участников форума *Carderplanet*. По словам одного из моих собеседников, Левашов — в отличие от других людей из киберподполья — вплоть до конца 2000-х продолжал пользоваться ICQ, но его не арестовали, хотя мессенджер к тому времени принадлежал *Mail.ru* и спецслужбы легко могли получить к нему доступ.

Сам Severa рассказывал [95], что занимается спамом с 1999 года, и называл [96] себя «одним из самых живучих спам-королей интернета». За миллион рекламных доставленных писем он просил 200 долларов; за миллион писем с фишингом — 500 долларов. Ему поступало до пятнадцати заказов в день. «Я заинтересован в крупных клиентах и активно стимулирую это большими скидками. Чем больше объем заказа, тем больше скидка», — писал он. Как и другие киберпреступники, Левашов почти никогда не работал в России, объясняя это «делом принципа»: «Сорри, это моя Родина». Когда в 2014 году началась война на Донбассе, хакер объявил, что вводит 30 % скидки на рассылки по Украине, США, странам ЕС и «прочим, кто ввел санкции»: «Для получения данной скидки необходимо ДО оплаты заказа назвать пароль: „Спасите жителей Донбасса от президента-пидораса“».

В начале апреля 2017 года Левашов вместе с женой и 4-летним ребенком отдыхал в Барселоне. Однажды ночью к ним в апартаменты, взломав дверь, ворвались полицейские и положили всех на пол. Левашова арестовали и обвинили в создании ботнета.

Жена Левашова рассказывала [97], что во время обыска сотрудники спецслужб отобрали у них все электронные устройства и заявили, что задерживают хакера из-за того, что «вирус, который якобы создал мой муж, связан с победой Трампа на выборах». Она же заявила, что у семьи никогда не было «сумасшедших денег», а Левашов — никакой не хакер: компьютер он использовал в основном для игр.

Из Барселоны Левашова перевезли в Мадрид, где он предстал перед судом и рассказал, что десять лет работал на партию «Единая Россия», собирая информацию про российскую оппозицию. Левашов заявил, что боится экстрадиции в США: «Меня подвергнут пыткам, в течение года я буду убит или покончу с собой, [они] хотят получить информацию военного характера и про партию „Единая Россия“».

«Единая Россия» отрицала сотрудничество с Левашовым, а МИД добивался того, чтобы хакера не выдавали США, обвиняя [98] американские власти в том, что они действуют «исподтишка», задерживая россиян, когда те выезжают за границу. Ведомство пыталось добиться экстрадиции хакера в Россию, мотивируя это тем, что в 2014 году он взломал [99] компьютеры одной санкт-петербургской



больницы, но испанский суд в итоге удовлетворил запрос американского правительства. В феврале 2018 года хакера перевезли в США.

Там Левашова обвинили вовсе не во взломах в пользу российского государства, а в создании ботнета *Kelihos*, в который входило более 100 тысяч зараженных компьютеров. Американские власти считают, что ботнет использовался не только для спама, но и для DDoS-атак и похищения данных с зараженных устройств.

Российское посольство в США заявило, что «глубоко обеспокоено ситуацией с Петром Левашовым, который стал очередной жертвой „охоты“ американских спецслужб за россиянами по всему миру». Дипломаты, посетившие хакера в тюрьме, рассказали, что с ним жестко обращаются: «Российский гражданин был помещен в маломерную одиночную камеру размером два на два метра, в которой практически отсутствует освещение. В камере подвергается постоянному шумовому воздействию, исходящему со стороны соседних помещений. По этой причине, а также из-за отсутствия подушки и матраца он лишен полноценного сна. Кроме того, ему запрещены общение с другими заключенными, прогулки на свежем воздухе, а также телефонные звонки родственникам в Россию».

В США Левашов признал себя виновным в мошенничестве и преступлениях в сфере компьютерной безопасности и хищении личных данных. Ему грозит до 50 лет заключения, приговор вынесут осенью 2019 года.



# Часть III

## Власть

### Глава 19

#### Медвежонок из КГБ

3 июня 1989 года в лесу под Ганновером в Германии нашли [\[100\]](#) сожженное тело неизвестного мужчины. Оно лежало около заброшенного и пыльного автомобиля, который выглядел так, будто простоял в этом лесу несколько лет; рядом валялась пустая канистра для бензина. На мужчине не было обуви — ее так потом и не нашли.

Вскоре полиция сообщила, что погибший — 24-летний житель Ганновера Карл Кох. О том, что он исчез, сообщил начальник Коха, когда его подчиненный не вернулся на работу после обеденного перерыва. Полиция посчитала смерть самоубийством — и вряд ли бы это привлекло внимание журналистов, если бы не тот факт, что Кох был фигурантом громкого судебного процесса. Его подозревали в работе на КГБ.

Кох был участником хакерской группировки, которая годами взламывала системы Минобороны США, NASA и других американских ведомств. Со взломанных компьютеров они скачивали документы, а их и доступ к системам продавали сотрудникам КГБ в Восточном Берлине за деньги и наркотики.

Когда Кох учился в школе, он прочитал книжную трилогию *The Illuminatus!* — в ней увлекательный фантастический сюжет был завязан на конспирологические теории о мировом заговоре. Став компьютерщиком, он взял себе ник Капитан Хабард в честь одного из героев этих романов. Кох был убежден, что и компьютерные сети — тоже ловушка иллюминатов, тайно управляющих миром, а за ним самим, как и за Хабардом, наблюдают инопланетяне.

И Кох, и его приятели стали первым поколением, которое начало использовать и первые персональные компьютеры, и интернет, который уже начинал походить на нынешний. В начале 1980-х компьютеры начали использовать не только для военных или программистских нужд, но и просто дома: например, для учебы, ведения семейного бюджета и, конечно, видеоигр, вроде *Space Invaders* или *Arkanoid*. В 1981 году IBM выпустил первый PC, Apple выпустил первый *Macintosh*. Появлялись и более дешевые компьютеры вроде *ZX Spectrum*, на которых можно было как раз начинать программировать. В те же годы возникли и протокол обмена данными TCP / IP, и система распределения доменов DNS, и распределенная система WWW — все составляющие нынешнего интернета.

Тогда же начали появляться не только первые хакеры, но и объединения. В 1981 году в Германии некоторые из них объединились в *Chaos Computer Club* — его участники собирались [\[101\]](#) менять общество с помощью новых цифровых технологий.



В какой-то момент Кох начал много общаться с людьми из *Chaos Computer Club*. Одному из новых знакомых он рассказал, что придумал такой способ самоубийства: построить атомную бомбу, взобраться на одну из башен всемирного торгового центра в Нью-Йорке и — взорваться.

В те же годы, в середине 1980-х, Кох сочинил манифест, в котором предсказывал, что в ближайшем будущем начнутся информационные войны с использованием «мягких бомб» — компьютерных вирусов. На тусовках он часто рассказывал незнакомым людям, что он самый серьезный и талантливый хакер современности.

Вскоре Кох познакомился с *Pengo* — подростком, фанатевшим от киберпанк-романа Уильяма Гибсона «Нейромант», герой которого ворует информацию из компьютерных сетей. В 1984 году шестнадцатилетний *Pengo* перестал обращать внимание на учебу и своих друзей, бросил работу в салоне видеоигр и стал все основное время проводить со своим компьютером и модемом.

\*\*\*

В последние годы холодной войны многие предчувствовали скорые изменения, но формально США и страны НАТО оставались врагами СССР. В 1986 году Кох, *Pengo* и их друзья задумались о том, чтобы зарабатывать на взломах, — и решили заняться компьютерным шпионажем для стран Восточного блока. Свою группировку они назвали *Equalizer*, имея в виду, что, продавая советским властям военную и научную информацию, уравнивают шансы в их противостоянии с западными странами, а значит, укрепляют мир во всем мире.

В сентябре 1986 года в здание советского посольства на улице Унтер-дер-Линден в Восточном Берлине приехал один из членов группировки — Питер Карл. На входе он сказал охраннику, что хотел бы поговорить об одном деле с кем-то из КГБ. Охранник предложил подождать, через полчаса к хакеру вышел мужчина и спросил, в чем дело. Тот объяснил, что он и его приятели могут получить доступ к системам с самой секретной информацией в мире и предоставить СССР технологии, которые помогут обогнать Запад. К тому моменту хакеры уже подготовили для КГБ «демонстрационный пакет»: они получили доступ к информационным системам министерств энергетики и обороны США и записали на дискеты некоторые секретные документы, например, перечень всех компьютеров, имевшихся к тому моменту на территории США. Выслушав Карла, сотрудник КГБ кивнул и удалился — а еще через десять минут к немцу вышел другой мужчина, представившийся Сергеем. По воспоминаниям Карла и его компаньонов, Сергей не очень понимал, что означает слово «хакер», но предложил им привезти ему примеры украденных документов, чтобы отправить их на экспертизу в Москву. Между собой хакеры прозвали сотрудника КГБ *Teddy Bear*.

К концу 1980-х советские спецслужбы еще не успели вырастить своих специалистов по компьютерной безопасности и атакам; судя



по всему, эта встреча была первым опытом их сотрудничества с хакерами и сотрудники КГБ не очень понимали их возможности. Когда один из членов группировки предложил провести семинар по хакингу для советских спецслужб, Сергей сказал, что его это не интересует.

Следующие встречи с КГБ проходили раз в неделю. Хакеры показали Сергею список компьютеров, к которым они могли получить доступ; *Teddy Bear* в ответ сообщил пожелания своих работодателей: им нужны были документы о радиотехнике, ядерном оружии и Стратегической оборонной инициативе — долгосрочной программе противоракетной космической обороны, объявленной президентом США Рейганом в 1983 году. В целом КГБ интересовали любые документы с компьютеров Минобороны США; кроме того — разработки американских операционных систем.

Большую часть времени друзья-хакеры просто «серфили» по сетям в поисках интересной информации. Проникая в системы, они искали по словам «*nuclear*», «SDI» («Стратегическая оборонная инициатива» — система противоракетной обороны США. — Прим. Авт.), «*star wars*», «*missile*». Некоторые из документов, которые хакеры передавали КГБ, находились простым поиском в интернете того времени, но советские чиновники платили [\[102\]](#) и за них: слово «Пентагон» было для них волшебным.

На следующих встречах, даже когда хакеры ничего не приносили, Сергей выдавал им 600 немецких марок (300 долларов) и подарки вроде банки икры или красивой зажигалки. Одному из них он передал фотографию девушки, чтобы показать полиции, если у него будут спрашивать, к кому он так часто ездит в Восточный Берлин.

Хакеры передали КГБ доступ к базам данных Пентагона и NASA, ядерной лаборатории в Лос-Аламос, а также материалы о космической, ядерной инфраструктуре Западной Германии, Франции, Японии, Великобритании. Среди прочего группировка взломала системы ядерного исследовательского центра CERN в Женеве. За передачу данных КГБ они получили несколько сотен тысяч долларов.

В 1988 году спецслужбы США совместно с программистом Клиффордом Столлом, который первым заметил проникновение в систему компьютеров библиотеки американского университета, в которой он работал, обнаружили, что хакеры получили доступ к 30 компьютерам в военных ведомствах. Они вышли на след взломщиков, и вскоре спецслужбы ФРГ задержали хакеров в нескольких немецких городах. На время суда их не стали помещать под арест.

Несмотря на загадочную смерть Коха, суд прошел спокойно. Главным свидетелем стал один из членов группировки — *Pengo*. Он дал подробные показания и пошел на сделку со следствием. Подростка амнистировали, другие хакеры получили условные сроки и штрафы. Рассматривая дело, судья заметил, что советские спецслужбы, видимо, просто не поняли, какие возможности могли им предоставить хакеры. Тем не менее немецкий телеканал ARD оценил [\[103\]](#) действия хакеров как самый серьезный случай шпионажа



с 1974 года, когда обнаружилось, что помощник канцлера ФРГ был восточногерманским шпионом.

Знакомые Коха не считали его смерть самоубийством: одних [\[104\]](#) удивляло, что трава вокруг тела сгорела по аккуратному кругу; других [\[105\]](#) — то, что хакер вообще поехал с канистрой бензина в лес за 70 километров от дома, вместо того чтобы покончить с собой более простым способом.

Со временем история Коха превратилась в своего рода хакерскую легенду — на форумах его иногда называют [\[106\]](#) «великим воином». Историю немецкой группировки в начале 1990-х рассказал Джон Маркофф в своей книге «Киберпанки». Это была одна из немногих книг о хакерах, которую перевели на русский и распространяли в интернете в середине-конце того десятилетия. Любой киберподпольщик того времени, задумывавшийся о сотрудничестве с государством, наверняка знал эту историю.



## Глава 20

### Хакеры-патриоты

Через 25 лет после загадочной смерти Карла Коха бывший сотрудник КГБ Владимир Путин, работавший в ГДР в те же годы, когда его ведомство сотрудничало с хакерами, заговорил о хакерах-патриотах. Так совпало, что поводом для этого стал вопрос, который во время Петербургского экономического форума в 2017 году президенту России задал немецкий журналист.

— В Германии довольно нервно реагируют на сообщения о возможных хакерских взломах со стороны России и о том, что российские хакеры могут начать манипулировать избирательным процессом, — сказал Питер Кропп, представитель крупнейшего немецкого агентства DPA. — Что вы об этом думаете?

— Хакеры — свободные люди! — ответил Путин. — Как художники. Настроение у них хорошее — они встали с утра и картины рисуют. Так же и хакеры: они проснулись сегодня, прочитали, что там что-то происходит в межгосударственных отношениях, если они настроены патриотически, они начинают вносить свою лепту, как они считают правильным, в борьбе с теми, кто плохо отзывается о России. Теоретически это возможно. На государственном уровне мы этим не занимаемся, вот что самое важное. Могу себе представить и такое, что кто-то специально это делает, выстраивает цепочку атак таким образом, чтобы источником этой атаки представить территорию Российской Федерации. Ведь современные технологии позволяют это делать, это достаточно легко делается.

Высказывание президента России в чем-то напоминало комментарий Дональда Трампа о попытке российских хакеров повлиять на американские выборы: Трамп заявил, что взломать структуры Демократической партии США мог «какой-нибудь человек весом 180 килограммов, сидящий у себя дома на диване».

— Я глубоко убежден, что никакие хакеры не могут кардинально повлиять на ход избирательной кампании в другой стране, — добавил Путин, прижав руку к сердцу. — Это не ляжет на сознание избирателей, сознание народа, никакая информация не ляжет и не повлияет на конечный результат.

Риторика Путина не меняется с годами и не зависит от того, какими доказательствами подкрепляются обвинения в том, что хакерские атаки организует Кремль. В 2016 году, когда эти обвинения только начались, президент отвечал [\[107\]](#) на них почти теми же словами. «Знаете, сколько хакеров сегодня? Причем они действуют настолько филигранно, настолько тонко, могут показать в нужном месте и в нужное время свой след — или даже не свой след, а замаскировать свою деятельность под деятельность каких-то других хакеров из других территорий, из других стран, — говорил он. — На государственном уровне мы этим точно не занимаемся».

Это не совсем так. В последние годы Россия активно занимается разработкой кибероружия и систем киберзащиты, а также рекру-



тирует хакеров для различных задач. А хакеры-патриоты, которые успешно помогают государству решать его геополитические задачи во время военных конфликтов, начали действовать еще десятилетия назад.

\*\*\*

В августе и сентябре 1999 года в Москве и Волгодонске взорвали несколько жилых домов — погибли 307 человек, около 1700 пострадали. В случившемся обвинили чеченских террористов: в том же августе 1999-го отряды боевиков под руководством Шамиля Басаева начали боевые действия на территории Дагестана, чтобы освободить регион «от оккупации неверными».

Вскоре российские войска блокировали границы Чечни, а 30 сентября (через неделю после того, как президент Борис Ельцин подписал указ о проведении «контртеррористической операции» — КТО) вошли на территорию республики. «Операция», которую на официальном уровне так и не называли войной, продолжалась следующие десять лет: формально режим КТО был отменен только в апреле 2009 года.

Вторая Чеченская оказалась первым конфликтом, в котором российские хакеры встали на сторону государства и фактически воевали с противником. Пока после взрывов в жилых домах в большинстве российских городов люди дежурили у своих подъездов, высматривая подозрительных незнакомцев у подвалов, другие решили бороться с врагом активно — но не покидая собственных домов и городов.

Несколько студентов Томского политехнического университета организовали [\[108\]](#) «Сибирскую сетевую бригаду». Она проводила DDoS-атаки на сайты чеченских боевиков, где те публиковали свои новости и интервью, причем киберактивисты начали действовать еще до того, как конфликт перешел в активную фазу. 1 августа 1999 года на главной странице сайта kavkaz.org они разместили [\[109\]](#) рисунок — на нем был изображен поэт Михаил Лермонтов в камуфляже и с автоматом Калашникова. «Здесь был Миша, — сообщала подпись в цветах российского флага. — Этот сайт террористов и убийц был закрыт по многочисленным просьбам россиян».

Участники «Бригады» также посылали письма в американские хостинг-компании с требованием больше не предоставлять свои услуги террористам. 17 ноября 2001 года лидер организации отправил [\[110\]](#) в американские СМИ и Госдепартамент США очередное обращение. «События, произошедшие в вашей стране 11 сентября 2001 года, сблизили позиции наших государств в вопросах борьбы с международным терроризмом, — сообщал он. — Компания XO Communications, Inc. предоставляет услуги хостинга информационному агентству „Кавказ-центр“, принадлежащему лицам, признанным международными террористами, в том числе и в вашей стране. Данный сайт используется не только для размещения материалов, дис-



кредитирующих усилия мирового сообщества по борьбе с международным терроризмом, но и для вербовки новых боевиков и сбора денежных средств для террористов». Через месяц ресурсу отказали в хостинге, и «Кавказ-центр» переехал на грузинские серверы (не в последний раз: после этого сайту приходилось переезжать [\[111\]](#) в Эстонию, Латвию и Финляндию).

В 2002 году хакеры-патриоты из «Бригады» снова взломали сайт «Кавказ-центра», оставив на его главной странице сообщение. «Мы вырвали жало из вонючей пасти „Гавгав-центра“, и над логовом чеченских террористов повисла тишина. Захлебнулся лаем удугов (имеется в виду Мовлади Удугов, в тот момент руководитель «Кавказ-центра» и министр информации самопровозглашенной Ичкерии. — Прим. Авт.). Замолчал в горах бандитский автомат. Не отправил чеченским наемникам деньги хитрый араб. Загрустил злой талиб в Афгане. Если завтра эту пасть заткнете вы, мир станет еще спокойнее и еще безопаснее».

Участники «Бригады» открыто призывали коллег также атаковать ресурсы боевиков: «Награда лучшим — восхищение братьев по online-цеху и счастливое, залитое солнцем завтра». Через несколько месяцев русскоязычные хакеры начали [\[112\]](#) массово распространять вирус *Masyanya*, названный в честь популярного в тот момент интернет-мультфильма: он был безвреден для пользователей, но по его команде зараженный компьютер становился участником DDoS-атаки на «Кавказ-центр».

Руководитель «Кавказ-центра» Мовлади Удугов был уверен [\[113\]](#), что за действиями хакеров стоит ФСБ. В томском ФСБ публично говорили [\[114\]](#), что «Сибирская сетевая бригада» не нарушает российское законодательство, а действия ее участников «являются выражением их гражданской позиции, которая достойна уважения», — несмотря на то что в тот момент уже существовала 272-я статья Уголовного кодекса о неправомерном доступе к компьютерной информации.

Еще через несколько месяцев, 23 октября 2002 года, боевики захватили московский театральный центр, где показывали мюзикл «Норд-ост». Сайты террористов снова были взломаны. После этого «Сибирская сетевая бригада» перестала проводить свои акции; чем ее участники занимались в последующие годы, неизвестно.

\*\*\*

В 2005 году в истории хакеров-патриотов началась новая эпоха — именно тогда на профильных форумах стали появляться призывы объединиться, чтобы атаковать экстремистские ресурсы.

Одним из тех, кто их распространял, был тот самый *Petr Severa* — король спама, которого в 2017 году арестуют в Испании. Например, он рекомендовал товарищам по киберподполью вступать в «Гражданский антитеррор» — сообщество, которое весной 2005 года создали [\[115\]](#) некоторые хакеры-патриоты. Они опубликовали мани-



фест о том, что самое важное оружие в XXI веке — это информация. «Наша цель — перекрыть доступ к информационным ресурсам, размещающим искаженную информацию о терроризме и террористах, пропагандирующим правильность их действий, на чем бы она ни основывалась, — заявляли они. — Террористические организации могут себе позволить прекрасных специалистов, обеспечивающих безопасность своих ресурсов. Мы уважаем их профессионализм — но не понимаем, как можно продать свою совесть». Действовали они теми же методами, что и предшественники, — с помощью DDoS-атак.

Через месяц появился [\[116\]](#) другой похожий проект — *Internet Underground Community vs. Terrorism*. Его сайт был оформлен в черносиних тонах: в шапке сайта друг другу противостояли хакер и человек в куфии (мужском головном платке, популярном в арабских странах). Создатели проекта указывали [\[117\]](#), что ищут DDoS-специалистов, и отрицали связь с российскими властями и спецслужбами, утверждая, что проект был задуман людьми, находящимися «по ту сторону закона». В разделе «Программы» на сайте проекта было выложено средство для DDoS-атак; там же размещалась своего рода доска почета — таблица, в которой были указаны атакованные ресурсы и время, в течение которого они не работали.

После нападения [\[118\]](#) боевиков на Нальчик в октябре 2005 года хакеры атаковали не только «Кавказ-центр», но и СМИ, которые, по их мнению, неправильно рассказывали о действиях террористов: «Эхо Москвы», «Новую газету», «Радио Свободу». Еще через месяц они сломали сайт Национал-большевистской партии (запрещена в России) Эдуарда Лимонова — на следующий день после этой атаки Верховный суд как раз ликвидировал межрегиональную общественную группу НБП.

После этого DDoS-атаки на оппозиционные и протестные сайты стали все более частыми. Весной 2007 года дискуссия вокруг переноса памятника советским солдатам, погибшим во Второй мировой войне, из центра Таллина на военное кладбище переросла в международный конфликт: МИД РФ вручил послу Эстонии ноту протеста, у посольства Эстонии в Москве проходили пикеты прокремлевского движения «Наши».

В этот момент хакеры атаковали сайты президента Эстонии, премьер-министра, госучреждений, банков — из-за DDoS-атак они перестали открываться на несколько недель. На главной странице правящей Реформистской партии появилось обращение, которое, по мнению хакеров, должен произнести глава партии и председатель эстонского правительства Андрус Ансип, — в нем он просил прощения у русского населения страны и обязывался вернуть памятник на место. Один из атакованных банков потратил [\[119\]](#) на восстановление от атаки около 10 миллионов евро. В докладе *Elliot School of International Affairs* атаки называли [\[120\]](#) «первой мировой кибервойной».



Ответственность за организацию атак взял [\[121\]](#) на себя комиссар движения «Наши» Константин Голоскоков. «Не называл бы это атакой, скорее киберзащитой, — говорил [\[122\]](#) он. — Эстонский режим получил урок». Спецслужбы США считают [\[123\]](#), что бот-сетью атаки управлял все тот же *Petr Severa*.

Примерно тогда же петербургскому программисту Антону Москалю позвонил неизвестный. Как рассказывал [\[124\]](#) журналист Андрей Солдатов, мужчина представился сотрудником Национального антитеррористического комитета ФСБ. Он спросил, действительно ли Москаль владеет сайтом «Гражданский антитеррор». Сайт Москалю на деле не принадлежал — он только сделал его зеркало у себя в блоге. Сотрудник ФСБ «завел с программистом разговор о патриотизме и борьбе с сайтами террористов». Узнав, что позвонил не тому, он спросил, как связаться с хакерами, работающими над проектом.



## Глава 21

### Остановить Грузию

8 августа 2008 года хакер Леонид Стройков — в интернете он чаще всего подписывался как *R0id* — сидел дома, в своей хабаровской квартире, пил пиво и читал юмористический сайт «Башорг». В какой-то момент его внимание привлек экстренный выпуск новостей по телевизору: там сообщали, что грузинские войска начали обстреливать столицу Южной Осетии Цхинвали (Южная Осетия формально была частью Грузии, но у властей региона был давний вялотекущий конфликт с Тбилиси).

В ночь на 8 августа 2008 года Грузия начала обстреливать Цхинвали, столицу Южной Осетии. Перед артиллерийской атакой с обеих сторон происходили перестрелки в приграничных селах. Грузинские войска на день заняли город. Почти сразу же на российских телеканалах начали говорить о тысячах жертв и о «геноциде осетинского народа». После этого конфликт стремительно перерос в пятидневную войну между Грузией и Россией. Российские войска, подошедшие из Владикавказа, выбили грузинских солдат из Цхинвали. По данным Следственного комитета России, во время августовских событий 2008-го погибли 162 жителя Южной Осетии и 54 российских военных; со стороны Грузии, по некоторым данным, погибло до 397 человек (большинство — гражданские); тысячи грузин переехали в поселки беженцев.

Впечатлившись услышанным, опытный хакер Стройков (в 2006 году он, например, подробно рассказывал [\[125\]](#), как взломать онлайн-банк) начал изучать сайты грузинских правительственных организаций и СМИ — искать дыры в защите, через которые можно их атаковать. Вскоре были взломаны несколько сайтов грузинских СМИ. Потом Стройков обратил внимание на государственные ресурсы. Вскоре на главной странице грузинского парламента появились фотографии грузинского президента Михаила Саакашвили, на которых он сравнивался с Гитлером. «И кончит он так же... — гласила подпись. — *Hacked by South Ossetia Hack Crew*».

«Ни одно крупномасштабное событие не обходится без участия СМИ, они активно используют интернет для передачи своего видения происходящего, публикуют исключительно то, что хотят, или то, что подсказали, — писал позже Стройков. — Абсолютно противоположные взгляды российских и западных / грузинских изданий побудили меня глубже вникнуть в ситуацию, со всеми вытекающими отсюда последствиями:»». О своей атаке на Грузию он подробно рассказал журналу «Хакер», сообщив, что «кибервойны стали неотъемлемой частью реальных кровопролитных событий».

Стройков был не единственным хакером, который «глубже вник в ситуацию». 9 августа — на следующий день после того, как Россия ввела свои войска на территорию Грузии, — появился сайт [stopgeorgia.ru](#). Там были размещены [\[126\]](#) рекомендации о том, какие грузинские сайты атаковать, ссылки на необходимые про-



граммы и советы новичкам. На форуме сайта было около 30 постоянных участников — в основном хакеры, которые зарабатывали кардингом; призывы поучаствовать в проекте появлялись на форуме журнала «Хакер» и других площадках для общения хакеров — exploit.in, zloy.org, web-hack.ru.

Создатели сайта представлялись «представителями русского хак-андеграунда». «Не потерпим провокации со стороны Грузии в любых ее проявлениях, — заявляли [127] они в своем обращении. — Мы хотим жить в свободном мире, а существовать в свободном от агрессии и лжи Сетевом пространстве». Они обещали атаковать грузинские ресурсы «до тех пор, пока ситуация не изменится» и призывали помочь «всех, кому не безразлична ложь политических грузинских сайтов». На *Stopgeorgia* появился [128] список «первоочередных целей» для атак — после этого перестали работать сайты грузинского президента, парламента, МВД, Минобороны.

Случались [129] в те дни и кибератаки на российские ресурсы: нападали на РИА «Новости» и другие российские и осетинские СМИ; сайт *Russia Today* в результате DDoS-атаки не работал около часа. Кто-то создал сайт с фальшивыми новостями, выглядевший как осетинское информагентство.

На хакерских форумах атаки на Эстонию и Грузию в основном поддерживали: «респект „нашим людям“»), «нужно ддосить и дефейсить эстонские сайты с пропагандой против России!», «Главный критерий — эффективность. Какая разница подло или нет? Тем более в военное время».

*Stopgeorgia* продолжал действовать и после войны. Когда в декабре 2009 года грузинские власти демонтировали мемориал воинской славы в Кутаиси (на месте памятника советским солдатам собирались построить здание парламента), хакеры снова начали обрушивать грузинские государственные сайты. «Не потерпим уничтожения нашего исторического наследия и попыток столкнуть лбами народы бывшего СССР, — писали они в своем заявлении на одном из хакерских форумов. — Мы выступаем за мир и дружбу наших народов и не допустим разжигания межнациональной розни между людьми, чья история навеки скреплена узами братства».

Позже исследователи выяснили [130], что *stopgeorgia.ru* был зарегистрирован у хостера «Наунет», который отказывается выдавать данные о владельцах по запросу правоохранительных органов. Организация *Spamhaus* давно занесла эту компанию в черный список за то, что она предоставляет площадку спамерам и киберпреступникам. Здание компании «Наунет» находится неподалеку от Белорусского вокзала в центре Москвы: хостер делит его с НИИ «Эталон», близким государству предприятием, которое занимается производством систем информационной безопасности. В 2015 году «Эталон» стал частью «Ростеха» — госкомпании, где работает Василий Бровко, интересовавшийся программами и оборудованием для проведения DDoS-атак.



Указанные при регистрации сайта stopgeorgia.ru почта и телефон были неоднократно засвечены на форумах кардеров — они принадлежали некоему Андрею Угловатому, который продавал базы украденных кредитных карт, а также поддельные паспорта и водительские удостоверения (скорее всего, имя было вымышленным).

IP-адрес stopgeorgia.ru принадлежал небольшой компании *Steadyhost*, находящейся на Хорошевском шоссе, 88, — в районе Москвы, где почти все здания связаны с Главным разведывательным управлением Генштаба (ГРУ) [\*\*\*]. В соседнем здании — в доме 86 — находится 6-й НИИ Минобороны, центр военно-технической информации и исследования военного потенциала зарубежных государств, ранее подчинявшийся ГРУ. Местные жители называют это четырехэтажное здание, построенное в 1930 году, «Пентагоном» — не из-за формы, но из-за секретности; сотрудников НИИ характеризовали [131] как «самых информированных людей в ГРУ», а руководство института входит [132] в Совет безопасности России.

По словам нескольких русскоязычных хакеров, именно во время и после событий в Грузии российские спецслужбы стали сотрудничать с хакерами системно. С тех пор их привлекают к работе регулярно — иногда добровольно, иногда принудительно: под угрозой уголовных дел.

Как рассказывает один из моих собеседников, в спецслужбах предпочитают не держать в штате много технических специалистов, а курировать внештатных сотрудников: их находят через уголовные дела о взломах и кардинге или нанимают на подпольных профильных форумах. Бывший глава отдела расследований «Лаборатории Касперского» Руслан Стоянов, много сотрудничавший по работе с ФСБ, открыто предупреждал, что такое сотрудничество опасно. «Существует огромный соблазн для „людей, принимающих решения“ воспользоваться готовыми решениями российской киберпреступности в целях влияния на геополитику, — писал Стоянов, который с января 2017 года находится в СИЗО «Лефортово» по обвинению в госизмене, в своем открытом письме [133]. — Самый ужасный сценарий — дать киберпреступникам иммунитет от возмездия за кражу денег в других странах в обмен на разведданные. Если это произойдет, появится целый слой „воров-патриотов“. Полулегальные „патриот-группы“ могут гораздо более открыто вкладывать ворованные капиталы в создание более современных троянских программ, а Россия получит самое продвинутое кибероружие». На деле услугами таких «патриот-групп» в спецслужбах пользуются уже не меньше десяти лет.

Чем после грузинских событий занимался Леонид Стройков, неизвестно; судя по его нынешней странице во «ВКонтакте», Стройков любит камуфляжную одежду и ходит на охоту с ружьем. На мои вопросы он не ответил. В социальной сети у хакера 36 друзей, большинство из Хабаровска, где он по-прежнему живет. Исключение — Дмитрий Докучаев, сотрудник ФСБ, известный как хакер *Forb*. Докучаев был одним из первых хакеров, перешедших на постоянную ра-



боту в спецслужбы, а в 2016 году, возможно, курировал атаки на инфраструктуру Демократической партии США (подробнее о Докучаеве — в главе 31).



## Глава 22

### Хакеры против либералов

В следующие годы хакеры-патриоты переключились на внутренних «врагов». Весной 2013 года организация «Хомячки» атаковала сайты большинства либеральных медиа, которые, по их мнению, оскорбили память 9 Мая. «Сегодня день Победы, и в этот день мы особенно хотим, чтобы память людей, отдавших свои жизни за нашу родину, ничем не оскорблялась, чтобы не было всевозможных домыслов и подтасовки фактов. Именно по этой причине ряд сайтов электронных СМИ сегодня не работает», — заявили они. Организованные ими DDoS-атаки специалисты оценивали как крупнейшие в истории российского интернета. Российская полиция никак не среагировала на атаки и не расследовала их.

«Хомячками» оказались студенты из Санкт-Петербурга; одним из руководителей группировки, видимо, был [\[134\]](#) Максим Болонкин, окончивший технический вуз по специальности «Программист». В том же году на молодежном форуме прокремлевских движений на Селигере он подарил футболки «Хомячков» депутатам Госдумы. Вскоре его организация получила [\[135\]](#) президентский грант на 7 миллионов рублей для создания «всероссийского позитивного молодежного информационного пространства».

Хакеров интересовали не только «либеральные» СМИ, но и оппозиционные политики. Ночью 25 июня 2012 года в твиттере Алексея Навального одно за одним начали появляться сообщения: «Чуваки, я тут решил сделать признание», «Я вас обманывал, чуваки, на самом деле я сосу хуй у едра, за это мне дали место в совете директоров аэрофлота, такие дела», «Хомячки и ебанные бараны, я вас обманул, я работаю на Путина, получаю бабло у белковского, не обижайтесь на меня», «Секту имени самого себя я распускаю, деньги вам не верну, потому что они мне нужны, чтобы тусоваться в Мексике, а вы все идите нахуй», «Покайтесь, хомячки, покайтесь и примите жестокую правду — я вас наебал...», «Меня никто не ломал, просто я решил сказать вам, наконец, правду, но я понимаю, как вам сейчас тяжело...».

Подписчики Навального сразу поняли, что политика взломали; сам он предположил, что это произошло через компьютеры и айпады, которые незадолго до того у него изъяли во время обыска. При этом сам политик говорил, что поменял пароли через 20 минут после того, как у него забрали технику.

Ответственность взял на себя хакер Хэлл — анонимный активист, помимо прочего, верящий во всемирный еврейский заговор. Он начал взламывать аккаунты знаменитостей еще в 2000-х, когда главной российской соцсетью был «Живой журнал»: его жертвами становились писатель Борис Акунин, публицист Владимир Прибыловский, депутат Госдумы Виктор Алкснис, политик Валерия Новодворская. Иногда после взломов хакер менял аватары во взломанных аккаунтах на фотографию мушкетера д'Артаньяна в исполнении



Михаила Боярского и подписывался: «Вы все — пидорасы, а я — д'Артаньян».

Содержимое взломанных почтовых ящиков Хэлл публиковал [\[136\]](#) в своем блоге «Виртуальная инквизиция». Сам он описывал себя как «Джокера», который «всегда и на все сто процентов достигает того, чего он хочет», готов «ликвидировать» любого, кто встанет на его пути, и «использует любые существующие методики управления людьми». В своем блоге он писал на «олбанском» языке, специально коверкая русские слова и постоянно матерясь, а большинство постов заканчивал междометием «хехе».

Многие были убеждены, что Хэлл получает деньги от администрации президента или работает на ФСБ: его взломы были дерзкими, а атаковал он только оппозиционеров. Прибыловский вместе с журналистом Андреем Мальгиным после взлома их аккаунтов начали кампанию по поиску человека, стоящего за ником Хэлл. Хакер несколько раз упоминал, что учился в историко-архивном институте РГГУ. Расследователи отправились в архив университета и раздобыли там личные дела студентов, биографии которых примерно подходили под другие известные подробности о жизни Хэлла. Методом исключения они дошли до Сергея Максимова.

На форумах Хэлл иногда откликался на Сергея и представлялся Максимом. Оказалось, что Максимов много лет назад переехал в Германию — а блог Навального взломали [\[137\]](#) именно с немецкого IP. Прибыловский и Мальгин создали блог «*seryozha\_vyhodi*», где начали подробно деанонимизировать хакера. Хэлл в ответ говорил, что все детали своей биографии всегда придумывал на ходу, в том числе про учебу в РГГУ.

Вскоре Максимова арестовали немецкие полицейские по обвинению [\[138\]](#) во взломах и подделке документов — по подсказке активистов, разыскивавших информацию о нем. На суде он говорил, что действительно живет в Германии и когда-то пользовался ником Хэлл, но с хакером только переписывался. При обыске на его компьютере обнаружили тысячи писем Навального и его жены, скриншоты его блога, записную книжку с IP-адресами — при этом никаких хакерских программ у Максимова установлено не было.

Прокуратура требовала посадить Максимова на два года; суд приговорил его к полутора годам условно и общественным работам. Никто из официальных российских лиц за него так не заступился. Хэлл вскоре вернулся к ведению блога — как и раньше, раз в несколько недель, он пишет посты о Навальном, которые, кажется, никто не читает.

В отличие от предыдущих взломов, последствия утечки переписки Навального оказались довольно серьезными. Политик считает, что уголовное дело по «Кировлесу» на него завели именно после публикации некоторых писем, в которых обсуждались связанные с компанией сделки (Навального и его партнера Петра Офицерова обвинили в хищении государственного имущества). Именно из-за при-



говора по «Кировлесу» Навальный не может баллотироваться в президенты.



## Глава 23

### Электричество кончилось

Война в Украине началась весной 2014 года, вскоре после нескольких недель антиправительственных протестов сторонников интеграции страны в Европу. Митинги закончились массовым расстрелом протестующих, в стране произошел переворот, президент Украины сбежал в Россию. После этого в городах Донбасса пророссийские активисты и военные начали захватывать административные здания; российские войска инкогнито высадились в Крыму и в итоге «присоединили» полуостров к России. Параллельно с этим связанные с российскими войсками хакеры начали тестировать в Украине кибероружие.

В мае 2014 года, накануне президентских выборов, хакеры [атаковали](#) ЦИК Украины. Организация, называвшая себя «Киберберкут» (аналитики связывали ее с российскими спецслужбами), блокировала работу сайтов МВД и Генпрокуратуры Украины, украинских телеканалов, взламывала почтовые ящики украинских политиков. Российских хакеров также обвиняли [\[139\]](#) во взломе приложения для расчета баллистических траекторий, которым пользовались украинские артиллеристы, — из-за этого войска потеряли до 80 % гаубиц; видимо, из-за ошибки в траекториях могли погибнуть и люди, невольно ставшие жертвами хакерских атак.

Самый же серьезный эпизод в кибервойне произошел в конце декабря 2015 года — вскоре после того, как на некоторое время остался без света присоединенный Россией Крым.

Днем 23 декабря оператор одного из центров управления энергетическими подстанциями Ивано-Франковской области заметил [\[140\]](#), что курсор на его мониторе дернулся, хотя сам оператор ничего не делал. Курсор двинулся в сторону переключателя, отвечающего за рубильник на одной из подстанций, и отключил его. Оператор попытался исправить положение, но компьютер его не слушался; потом его и вовсе выкинуло из системы управления подстанциями. Вскоре во всей Ивано-Франковской области исчезло электричество.

Как считает специалист по безопасности Роберт Ли из компании *Dragos Security*, ко взлому хакеры готовились не меньше полугода. Сначала они внедрили на компьютеры программу *Blackenergy 3*. Для этого они использовали проверенный способ: пользователям сети отправляли фишинговые письма с файлами *Microsoft Word*, которые при открытии предлагали установить макрос. Тот, в свою очередь, устанавливал вредоносную программу.

Внутренние сети распределительных центров были хорошо отделены от системы управления подстанциями при помощи файрволов. Журнал *Wired* отмечал, что эта защита лучше, чем та, что стоит в компаниях, управляющих американскими электросетями. Тем не менее хакерам удалось ее взломать — они получили данные обычных пользователей и могли при подключении притворяться ими.



На изучение того, как устроена сеть распределительных центров и как она связана с системой управления подстанций, у злоумышленников ушло несколько месяцев. За это время они также написали новую прошивку для конвертеров на подстанциях, которые получают сигнал через интернет и передают его рубильникам. Как отмечают эксперты, это был первый взлом, когда хакеры сумели перепрошить само оборудование.

Начав атаку, хакеры отключили источники бесперебойного питания у двух из трех распределительных центров, в сеть которых у них был доступ. После этого они запустили гигантский поток звонков в колл-центр «Прикарпатьеоблэнерго», чтобы жители не могли сообщить об отключении энергии. Одновременно они отключили 30 подстанций и перепрошили там конвертеры таким образом, что операторы перестали видеть их состояние удаленно. Переключить рубильник стало возможно только руками. На компьютерах операторов хакеры запустили программу, которая сделала невозможной перезагрузку.

Восстановить подачу света в регион удалось только через шесть часов, а возможность удаленно переключать рубильники восстановить так и не удалось — энергетикам придется заменить конвертеры, испорченные хакерами. *Wired* отмечает, что в США последствия такой атаки были бы куда серьезнее: там на подстанциях рубильники попросту нельзя переключить руками.

Украинские власти считают, что этой атакой стояла Россия. *Reuters* также указывал, что программу *Blackenergy* ранее использовали российские хакеры. Кроме того, название *Blackenergy* принадлежало группе хакеров, которая разработала вирусы массового поражения *Bad Rabbit* и *Petya*: они шифровали данные на зараженных компьютерах и требовали от пользователей выкуп за разблокировку. Так или иначе, специалисты, опрошенные *Wired*, не смогли точно сказать, кто организовал атаку на Ивано-Франковскую область: нельзя исключать варианта, при котором хакеры сначала взломали украинскую энергосистему, а потом продали свои наработки России.

\*\*\*

6 февраля 2016 года сотрудник исследовательской команды *Conflict Intelligence Team* Руслан Левиев засиделся у компьютера до ночи. Утром он собирался выпустить громкий материал. В нем рассказывалось [\[141\]](#) об участии российской 6-й танковой бригады из под Нижнего Новгорода в боях под Иловайском и Дебальцевом на Донбассе. Одним из доказательств участия российских военных в украинском конфликте была найденная Левиевым фотография, на которой министр обороны Сергей Шойгу награждает часами одного из раненых солдат в клиническом госпитале имени Бурденко в Москве. Публикацию Левиев проанонсировал в своем твиттере.

К тому моменту он уже привык публиковать тексты с серьезными обвинениями российских властей, которые отрицали присут-



ствие кадровых российских военных в Донбассе. Он чувствовал себя в относительной безопасности в своей московской квартире на юге Москвы, хотя ему не раз угрожали, а на улице он замечал слежку.

Последние годы Левиев сотрудничал с командой *Bellingcat* — она, используя открытые источники вроде выложенных в социальные сети фотографий, расследовала участие российских военных в конфликтах на Украине и в Сирии. Нидерландские власти использовали [142] данные *Bellingcat* в расследовании крушения малайзийского «Боинга», сбитого неподалеку от Донецка в июле 2014 года; в 2018 году именно *Bellingcat* сумели доказать, что обвиненные в отравлении российского перебежчика Сергея Скрипаля и его дочери Руслан Боширов и Александр Петров были агентами ГРУ, действовавшими под этими вымышленными именами.

Представляя уровень возможного внимания к себе, Левиев — на случай визита правоохранительных органов и отключения электричества — установил в квартире четыре запасных аккумулятора и продублировал подключение к интернету, дополнив связь по кабелю модемом «Йоты».

Около трех часов ночи Левиев продолжал перепроверять текст и верстку расследования. Рядом спали два кота — Котопус и Десантник. В этот момент экран мобильного телефона, лежавшего у Левиева на столе, засветился.

Левиев увидел, что ему пришли подряд несколько оповещений от твиттера, а через минуту — еще два оповещения от фейсбука. Во всех говорилось о попытках взлома аккаунтов. Левиев тут же поменял пароли в социальных сетях и начал проверять остальные аккаунты. С мессенджерами и рабочей почтой ничего не произошло, но хакерам удалось взломать почту Левиева на «Яндексе» — хотя как это получилось, он не понимает до сих пор: там стояла двухфакторная авторизация, привязанная к сим-карте «Мегафона».

С помощью взломанной почты хакеры восстановили доступ к «Живому журналу» Левиева и зашли через его аккаунт в административную панель *Bellingcat*. На странице Левиева в *Bellingcat* они разместили обращение: «*Bellingcat* — это про-НАТО и проамериканская организация провокаторов, они врут и шпионят, проблемы других — их хлеб. Они мусорщики, а не расследователи».

Ответственность за взлом взял [143] на себя «Киберберкут». Также хакеры получили доступ к *iCloud* Левиева — скачанные оттуда личные фотографии, сканы паспортов и домашний адрес расследователя они позже выложили на сайте «Киберберкута».

Американская компания *Threatconnect*, занимающаяся расследованиями киберпреступлений, подробно разобрала [144] атаки на Левиева и *Bellingcat*. Регулярно приходившие им фишинговые письма выглядели как оповещения *Google* о том, что в аккаунт жертвы вошел посторонний. Ссылки из письма переводили на фишинговые сайты. Домены, которые, по данным *Threatconnect*, использовались для атаки, немецкая разведка и аналитические компании называли



[\[145\]](#) среди принадлежащих *Fancy Bear* — группировки, которая примерно в то же время взломала сервера Демократической партии США. «По тому, как они действуют и какую используют инфраструктуру, можно понять, что „Киберберкут“ и *Fancy Bear* — это либо одна группа, либо просто соратники, действующие совместно», — сказал мне ведущий аналитик *Threatconnect* Рич Баргер.



## Глава 24

### Взломщики на госслужбе

Среди русскоязычных хакеров действуют несколько негласных правил. Об одном из них — «Не работать по ги» — я уже рассказывал. Другие гласят: если находишь во время взлома что-то, что может заинтересовать «режим», — делишься этим; когда тебя просят помочь из патриотических целей — ты соглашаешься. Отказ соблюдать эти договоренности означает уголовное преследование.

В начале 2001 года хакер UFO, которого вычислили спецслужбы, рассказывал [\[146\]](#), что после беседы со следователями ему предложил встретиться один из экспертов организации, близкой к спецслужбам, — он назвал его «Сидоровым». Через несколько месяцев после задержания хакер пришел домой и его мать, жившая вместе с сыном, сказала, что ему звонил неизвестный мужчина, который оставил свой телефон. Хакер перезвонил. «Сидоров» сообщил, что видел экспертизу по его делу и заинтересовался взломщиком.

Вскоре они встретились в московском ресторане, и «Сидоров» рассказал, что ему нужен сотрудник, чтобы заниматься тем, чем UFO занимался и так, — поиском уязвимостей. Платить мужчина обещал хорошо — и хакер согласился. Здание, где он должен был работать, оказалось «нехило оборудованным». Вскоре появились руководство: они спрашивали UFO, как обойти разные типы брандмаэуров, как вломиться в чужое TCP-соединение, как ввести удаленную систему в состояние «отказ в обслуживании». Хакер прошел этот тест. В течение следующих нескольких месяцев он прошел еще несколько тестов, его начали оформлять, но внезапно пришло новое руководство, которое решило не нанимать фрилансеров.

Сотрудник Центра информационной безопасности (ЦИБ) ФСБ — основного управления спецслужб, связанного с хакерской деятельностью, — рассказывал журналу «Хакер», что сотрудники приходят туда «реализовать свои убеждения». «Основное отличие ФСБ от любой коммерческой фирмы в том, что специалисты у нас не работают, а служат, и это очень важный момент, — говорил он. — При прочих равных условиях количество денег, которое может заработать один и тот же человек у нас и в серьезной коммерческой структуре, — разное. Работа в ФСБ — это не американский блокбастер из жизни неуловимых „бондов“, в нашей работе присутствует изрядная доля рутины, хотя кто-то находит и вполне романтические моменты».

Антон (имя изменено по его просьбе), занимающийся по основной работе анализом вирусов, периодически общается с сотрудниками ФСБ. По его словам, в ЦИБ мало технических сотрудников, поэтому они часто привлекают сторонних специалистов. «Существует распространенная схема по привлечению нелегальных хакеров, их поощрению, созданию для них условий для работы, чтобы через них получать нужную информацию», — объясняет хакер. По его словам, хакеров часто даже прячут на конспиративных квартирах, чтобы их



не поймали полицейские. Антон знает о нескольких случаях, когда людей задерживал отдел «К» МВД, а потом за задержанными приезжали сотрудники ФСБ и увозили их со словами: «Не ваше дело».

Некоторые из хакеров переходят на штатную работу в правоохранительные органы. Источники [\[147\]](#) *The New York Times* утверждают, что российский хакер Евгений Богачев, которого годами разыскивают американцы, сотрудничает со спецслужбами. Богачев создал сеть зараженных компьютеров по всему миру (кроме России), на которой заработал сотни миллионов долларов — атакуя и банки, и полицейские департаменты в Массачусетсе, и фирму, занимающуюся дезинсекцией в Северной Каролине. По словам собеседников издания, пока Богачев похищал деньги, «российские власти смотрели ему через плечо, изучая те же компьютеры в поисках файлов и электронных писем»: их якобы интересовала засекреченная информация на зараженных американских компьютерах о конфликтах на Украине и в Сирии; поиск осуществлялся по словам «совершенно секретно» или «министерство обороны».

«Говорят, [Богачев] живет припеваючи в Анапе и помогает эфэсбэшникам, — говорит мой источник, занимающийся анализом кибератак. — Почему нет? Если бы я был эфэсбэшником, я бы его, конечно, доил. Он в России, у него куча доступов, нельзя этим не пользоваться, но нужно помнить, что он преступник».

Весной 2012 года Антону дали очередное задание: взломать одно из главных российских информационных агентств. Заказчики требовали постараться: они боялись, что перед инаугурацией Владимира Путина злоумышленники «разместят на сайте бяку про Владимира Владимировича». Антон легко выполнил заказ — по его словам, никакой защиты от атак у агентства толком и не было: «Это была масса кода, написанная в начале 2000-х». Как обычно, он написал отчет о взломе и передал его руководству. Через год хакер из интереса решил проверить, как издание защитилось от дальнейших взломов. Все найденные им дыры в безопасности остались на месте.

По словам кибервзломщика, работающего на спецслужбы, часто ФСБ, наняв кого-то из хакеров, через него пытается подставить и заманить в ловушку его знакомых. Бывшая сотрудница отдела кибербезопасности ФБР Милана Патель рассказывала [\[148\]](#), что США и Россия долго проводили операции по поимке хакеров вместе, но потом ситуация изменилась: «Мы сообщали им о конкретном человеке, которого мы ищем, после чего он таинственным образом исчезал, чтобы позже объявиться уже на службе у российского правительства. По сути, сообщив ФСБ, на кого мы охотимся, мы помогли им набрать талантливых хакеров».

Российские спецслужбы, видимо, и сейчас продолжают вербовать хакеров в обмен на закрытие уголовного дела. В июле 2018 года в Белгороде суд прекратил [\[149\]](#) уголовное дело в отношении местного жителя, который совершил 545 кибератак на официаль-



ный сайт ФСБ. Дело было прекращено по ходатайству следователя ФСБ.

Источники в ФСБ найти почти невозможно. Их пресс-служба никогда не дает комментариев, публичные представители не отвечают на телефоны и почту, а выступают обычно только на закрытых мероприятиях.

В какой-то момент я отчаялся, но вспомнил правило, что 90 % времени репортер проводит в ожидании информации или в попытке ее достать. На очередной большой киберконференции, проходившей в Москве, я спросил у организаторов, как мне найти среди пришедших сотрудников спецслужб. Один из организаторов сказал: «Это те, которые ходят без бейджей». В следующем перерыве я вышел в лобби, и, бродя между столов, заваленных тартелетками, искал таких людей. В итоге я нашел троих, и только один согласился поговорить.

Он подтвердил, что хакеров просят консультировать спецслужбы по некоторым вопросам. По его словам, кибератаки на другие страны — не дело рук ФСБ: «Этим давно и успешно занимаются нанятые фрилансеры и кибервойска ГРУ».



## Глава 25

### Доктрина Герасимова

Начало 2010-х — важный водораздел в истории российских хакеров и государственных кибервойск. До того поручения властей выполняли отдельные криминальные хакеры или активисты; теперь государство собирало постоянные киберформирования при военных частях.

Первый серьезный документ [\[150\]](#) о кибервойне появился в конце 2011 года, когда Минобороны выпустило доклад «Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве». В нем рассказывалось, что ведомство не собирается вмешиваться во внутренние дела других стран, но будет поддерживать собственные кибервойска для безопасности и «готовности к отражению угроз военно-политического характера в информационном пространстве». В случае конфликта Минобороны оставляло за собой «право на индивидуальную или коллективную самооборону с применением любых избранных способов и средств».

Через два года один из кураторов ГРУ, генерал Валерий Герасимов, опубликовал [\[151\]](#) в журнале «Военно-промышленный курьер» материал, который позже станут называть «Доктриной Герасимова». В статье он описывал гибридную войну с применением кибервойск, например, для подрывной деятельности с целью подготовки поля боя перед интервенцией.

Новая доктрина фактически обновила российские разведывательные традиции. В предыдущую эпоху ГРУ занималось прежде всего внедрением своих агентов в нужные организации, а также вербовкой чиновников и сотрудников стратегически важных предприятий. Еще одним важным направлением деятельности ведомства была дезинформация — задолго до появления термина *fake news* разведчики и сотрудники КГБ распространяли фальшивки о том, что США применяли бактериологическое оружие в Корее в 1950-х, или о том, что американские спецслужбы заказали убийство Джона Кеннеди.

Важнейшим компонентом новых, гибридных методов ведения войны стали хакеры и кибервойска. Есть среди них и преемники людей, когда-то распространявших дезинформацию, — теперь сотрудники «фабрики троллей», которую связывают с российскими властями, пытаются расколоть американское общество с помощью постов и комментариев в фейсбуке (вплоть до публикации [\[152\]](#) негативных отзывов на последние «Звездные войны»).

Самая известная «фабрика» связана с Евгением Пригожиным — миллиардером, которого считают хорошим знакомым Владимира Путина (компании Пригожина годами получают многомиллиардные кейтеринговые госконтракты, в том числе на обслуживание приемов в Кремле). Первая «фабрика» находилась сначала в Ольгине (из-за этого их стали называть «ольгинскими ботами»), потом на



улице Савушкина в Санкт-Петербурге и официально называлась «Агентство интернет-исследований». Десятки сотрудников ежедневно приходили в это здание на работу, чтобы придумывать фейковые новости и писать (под вымышленными именами) комментарии в российских и зарубежных социальных сетях и форумах, хваля или ругая определенных политиков.

Одна из сотрудниц «фабрики» рассказывала [153], что ее смены длились по 12 часов. Перед каждой ей выдавали инструкцию: например, публиковать комментарии с оскорблениями в адрес президента Украины Петра Порошенко или писать, что российская оппозиция подстроила убийство Бориса Немцова.

В 2016 году главной темой для троллинговой активности снова стали США: там приближались президентские выборы, и сотрудники «фабрики» стали создавать в фейсбуке сотни сообществ и аккаунтов, так или иначе поддерживавших кандидатуру Дональда Трампа и агитировавших против Хиллари Клинтон. Например, в одном из постов сообщалось [154]: «Сегодня у американцев есть возможность выбрать президента с благочестивыми моральными принципами. Хиллари — Сатана, ее ложь и преступления доказывают, какое она зло. И даже если Дональд Трамп не совсем святой, в конце концов, он честный человек и он глубоко переживает за эту страну. Я отдаю свой голос ему!»

Сотрудники «фабрики», притворяясь американцами, даже организовывали в США митинги и собрания сторонников и противников кандидатов. Насколько все это повлияло на результаты выборов, которые в итоге выиграл Трамп, достоверно сказать невозможно. В феврале 2018 года американские власти предъявили 13 сотрудникам «Агентства интернет-исследований» обвинения во вмешательстве в президентские выборы; американский Минюст отмечал, что целью россиян было «посеять раздор в обществе».

В ноябре 2018 года американские кибервойска успешно [155] атаковали «Агентство интернет-исследований». В день выборов в Конгресс США американцам удалось отключить интернет в офисе «фабрики троллей», чтобы помешать им повлиять на голосование.

\*\*\*

Идею «научных рот», которые должны стать основой российских кибервойск, военные чиновники начали продвигать в 2013 году.

Незадолго до того министром обороны стал Сергей Шойгу. Сразу после назначения он начал проявлять интерес к кибербезопасности и высказываться о необходимости создания российских кибервойск — аналога американских *Cyber Command*, подведомственных Минобороны США и занимающихся военными кибероперациями и защитой американских компьютерных сетей. В июле 2013 года Шойгу объявил о начале «большой охоты» на молодых программистов. «Охоту в хорошем смысле этого слова, это продиктовано объемом программного продукта, который необходим армии



в ближайшие пять лет», — сказал [\[156\]](#) он на встрече с ректорами технических вузов, в которых есть кафедры информационной безопасности.

Какое конкретно применение найдут математикам и программистам, объяснил вице-премьер Дмитрий Рогозин, курирующий оборонзаказ. Он первым из российских чиновников заявил о создании киберкомандования. «Это связано с обеспечением информационной безопасности инфраструктуры государства», — сообщил [\[157\]](#) Рогозин. Источники указывали [\[158\]](#), что основными задачами российских кибервойск станут «обработка информации, поступающей извне, а также борьба с киберугрозами»; все служащие должны будут пройти лингвистическую подготовку и выучить английский язык.

Серьезность своих намерений Шойгу подтвердил в программе «Вести недели» через год после назначения — в октябре 2013-го, рассказывая о новых угрозах для России. Одной из таких он назвал кибероружие. «Оно, конечно, все ближе и ближе идет к понятию „оружие массового поражения“», — рассуждал министр обороны. — Мы уже вплотную подошли к тому, и это показывают хакеры разных стран, что за счет [кибероружия] можно добраться до чего угодно». По сути, Шойгу тогда повторил слова [\[159\]](#) президента Владимира Путина о «поражающей силе информационных атак», прозвучавшие в рамках его выступления на Совете безопасности за три месяца до того.

Весной 2014 года в Минобороны появились [\[160\]](#) «войска информационных операций» для «кибернетического противоборства с вероятным противником»; позже источники в Минобороны объяснили [\[161\]](#), что они созданы для «нарушения работы информационных сетей вероятного противника».

Их создали в формате «научных рот» в военных частях по всей стране. Набирать туда начали выпускников технических вузов — математиков, программистов, криптографов, инженеров. В анкете для поступления [\[162\]](#) просили указать знание языков программирования, программных сред. Новосибирский государственный технический университет объявлял [\[163\]](#) среди студентов набор в научную роту ЦНИИ Министерства обороны РФ в Сергиевом Посаде для участия в «применении суперкомпьютерных технологий». В сентябре 2015 года при Минобороны открылась кадетская школа [\[164\]](#) IT-технологий, а тремя месяцами позже Военную академию связи окончили [\[165\]](#) первые выпускники научной роты [\[166\]](#) «спецназа информационной безопасности».

Помимо студентов, Минобороны собиралось [\[167\]](#) призывать «имевших проблемы с законом хакеров». Один из руководителей киберрасследовательской компании *CrowdStrike* (она, в частности, расследует взломы, совершенные *Fancy Bear*), Дмитрий Альперович, подтверждал [\[168\]](#) эту информацию. «Когда замечают кого-то технически подкованного в российском подполье, на него заводится уголовное дело, потом он просто исчезает», — объяснял он.



В июле 2015 года во «ВКонтакте» появился рекламный ролик, призывающий записываться в кибервойска. На видео мужчина, перезарядив автомат, кладет его на стол рядом с ноутбуком. Потом начинает набирать на клавиатуре программный код. Под старомодный хард-рок поверх картинки появляется надпись: «Научная рота РФ». В видео, оформленном в духе фильмов про хакеров, мелькают фразы: «Если ты успешно закончил вуз, если ты специалист технических наук, если ты готов применить свои знания — мы предоставим возможность!» Заинтересовавшимся обещают работу на «мощных вычислительных комплексах».

Частично материалом для видео послужили кадры вирусного ролика [\[169\]](#) «Я — русский оккупант», герой которого саркастически «извиняется» перед зрителями за оккупацию Сибири, Прибалтики, Средней Азии и Украины: «Поймите: мне не нужна ваша лицемерная «свобода», мне не нужна ваша гнилая «демократия», мне чуждо все, что вы называете западными ценностями. Вежливо предупреждаю в последний раз: не нарывайтесь! Я строю мир, я люблю мир, а воевать я умею лучше всех».

Видео с агитацией за «научные роты» выложили в сообществе Межвидового центра подготовки и боевого применения войск радиоэлектронной борьбы под Тамбовом, при котором была создана одна из таких рот. Такое же видео появилось и на сайте научнаярота.рф. Почти карикатурная манера изображения киберсолдата чем-то роднила видео с сайтом *Fancy Bear* [\[170\]](#) — он принадлежит хакерской группировке, которую обвиняли в международных взломах в интересах России.

Один из преподавателей Тамбовского учебного центра Анатолий Балюков объяснял [\[171\]](#), что «основная задача наших ребят — изучать методы [кибератак] и поставить им надежный заслон». Помимо этого студенты должны были «отрабатывать алгоритмы кибератак, чтобы максимально эффективно воспользоваться ими при случае». В документах, выложенных в сообществе центра, указывалось, что в подразделении исследуют «уязвимости сетей, программного обеспечения».

Еще одна научная рота Генштаба находится [\[172\]](#) в Краснодарском крае. Как указано на сайте Минобороны, постоянно в ней находятся два взвода по 30 человек. Их распорядок [\[173\]](#) несильно отличается от армейского: подъем в 6 утра (исключение — воскресенье, в 7 утра); потом 50-минутная зарядка, завтрак; после 9 — «научная работа».

Желающим поступить в роту предлагалось заполнить анкету, где помимо вопросов по криптографии и математике спрашивали о родителях, желании создать что-то новое для Минобороны и об отношении к оформлению доступа к гостайне. После заключения контракта обещали офицерское звание и зарплату от 38 тысяч рублей. В брошюре, рекламирующей работу в научной роте, можно обнару-



жить фотографии «чайной комнаты» и «комнаты психологической разгрузки», сделанных в казармах для кибервойск: первая представляет собой комнату со столом, на котором стоят чайники, и развешанными по стенам пейзажами; вторая — гостиную с двумя диванами и аквариумом.

В ответ на запрос о посещении научной роты и интервью с военными представитель Минобороны позвонил мне и сообщил, что ведомство никому их не показывает и никому о них не рассказывает, «чтобы никто не мог узнать, как мы их можем применить». «Эта тема закрыта такими органами, как Федеральная служба... следующая буква «о» и ФСБ, — добавил представитель ведомства. — Не рискуйте дальше ничего делать, не ставьте на себе прицел».

Минобороны действительно никогда публично не рассказывало об устройстве кибервойск, их размерах и количестве сотрудников. При этом в изданиях, близких к министерству, и на сайте самого ведомства периодически появляются материалы об их достижениях.

Например, в сентябре 2014 года заместитель министра обороны Юрий Садовенко рассказывал [\[174\]](#) на встрече в рязанском воздушно-десантном училище о начале «освоения вопросов кибербезопасности». Минобороны сообщало [\[175\]](#), что в сентябре 2015 года российские военные на учениях «Щит Союза — 2015» отражали кибератаки с помощью системы обнаружения сетевых атак (СОА) — они выставляли программные фаерволы, которые фильтровали проходящие через компьютер сетевые пакеты.

Для продвижения научных рот телеканал «Звезда» выпустил в 2014 году 40-серийный сериал [\[176\]](#) «Ботаны» о новобранцах, попавших в кибервойска. В нем начальник генштаба Минобороны поручает начальнику одной из военных частей создать подразделение, которое будет заниматься кибероружием. В сериале звучат шутки вроде «за каждое подтягивание — час пользования интернетом». Телеканал «Звезда» анонсировал его так: «На завершающем этапе съемок стало известно, что в Министерстве обороны РФ было принято решение, что защитой российских военных систем связи и управления от кибератак различного характера будут заниматься специально созданные войска информационных операций».

Издание «Армия сегодня», освещающее деятельность Минобороны, сравнивало [\[177\]](#) работу научных рот с фильмами об агенте Джеймсе Бонде: «В последнем фильме компьютерный спец Кью протягивает агенту небольшой кейс и говорит: „Я могу доставить им больше неприятностей, сидя в пижаме перед ноутбуком, чем вы за год оперативной работы“. Вот таких специалистов хотят готовить в российских „кибервойсках“».

«Предполагать, что до 2014 года Россия не занималась проблемой своего присутствия в киберпространстве, довольно наивно, — сказал мне главный антивирусный эксперт «Лаборатории Касперского» Александр Гостев. — Вероятно, что для такой работы им требуются специалисты — именно поэтому и выбран формат „научной роты“».



Гостев передал мне фотографию страницы из буклета Минобороны. В нем под заголовком «Основные направления научной деятельности операторов научной роты главного управления ГШ ВС РФ» опубликована фотография солдат за компьютерами и указано, что их задача — «разработка специального программного обеспечения».

Примерно в начале 2014 года при Минобороны создали Центр специальных разработок. Сотрудников в него начали искать на сайтах вакансий среди выпускников технических университетов. Прежде всего требовались люди для анализа эксплойтов и «реверс-инжиниринга» (исследования механизмов работы программ и устройств для их последующего воспроизведения).

В вакансиях указывалось, что центр ищет сотрудников с «хорошими знаниями в области анализа исходных кодов различных программных продуктов для интересной работы в области ИБ (информационной безопасности. — Прим. Авт.)». Сотрудники получали форму допуска № 3 (с уведомительным порядком выезда за границу) и зарплату до 120 тысяч рублей. В объявлении указывалось, что офис находится в тихом районе — у реки на севере Москвы.

Как сказал мне источник в российской компании по защите информации, работать в российские кибервойска из коммерческих компаний ушли около сотни человек по всей стране.



## Глава 26

### Наука мракобесов

В России существуют десятки государственных научно-исследовательских институтов, связанных с Министерством обороны. Обычно они располагаются в неприметных серых конструктивистских зданиях вдалеке от пешеходных маршрутов. Во времена холодной войны в таких помещениях тысячи специалистов разрабатывали в том числе биологическое и химическое оружие — но не только его. Там же зарождались идеи и методы использования новых технологий в военных целях, которые десятилетия спустя аукнутся в современных киберконфликтах.

В середине 1950-х небольшое сообщество советских инженеров было взбудоражено выходом книги Анатолия Китова «Электронные цифровые машины». Фактически это была первая книга о программировании на русском языке, подробно рассказывавшая о внутреннем устройстве ЭВМ и о том, как эти машины могут использоваться в экономике, а в перспективе — и для создания искусственного интеллекта. Китов, которому тогда не было еще и сорока, моментально оказался главным советским пропагандистом кибернетики.

Он родился [\[178\]](#) в Самаре в 1920 году в семье офицера Белой армии и сотрудницы кондитерской. Чтобы поменьше попадаться на глаза большевикам, в 1921 году Китовы переехали в Ташкент и благодаря этому избежали голода в Поволжье, жертвами которого стали более 5 миллионов человек. Дорога была сложной: в России свирепствовал тиф, и трупы иногда лежали прямо на улицах; там же, под открытым небом, нередко приходилось ночевать. Когда Китов подрос, он начал увлекаться авиамоделированием, шахматами и математикой.

В пятом классе на уроке литературы Китов написал сочинение, которое назвал «Розовая сказка». В нем мальчик описывал свой сон: на центральном рынке в Ташкенте вместо пустых полок появились калачи, индейки, любые виды сыров, колбасы, одежды и обуви. Вскоре с пятиклассником пришли побеседовать двое сотрудников НКВД: они спрашивали, с чьей подачи Китов написал подобный издательский текст, но в итоге ушли ни с чем.

После школы Китов поступил на физико-математический факультет Ташкентского университета; он хотел заниматься ядерной физикой. Через два месяца его отправили на фронт: шла Великая Отечественная. В окопах он продолжал заниматься математикой и прошел материал первых двух курсов; в семейном архиве Китовых хранится конспект по высшей математике за 1944 год — когда его отряд вел тяжелые бои, освобождая украинский Самбор.

Вернувшись с войны, Китов переехал в Москву — учиться на баллистическом факультете в артиллерийской военно-инженерной академии имени Дзержинского; там же, окончив учебу, он начал работать научным референтом. Сергей Королев предложил ему перейти в его ракетное конструкторское бюро, но в это же время Китов



узнал о появлении первых ЭВМ и уговорил руководство академии послать его в качестве представителя Минобороны в специальное конструкторское бюро-245 (СКБ-245), где можно было получить доступ к секретным документам.

В спецхране Китов обнаружил книгу американского математика Норберта Винера «Кибернетика», написал по ее материалам статью о новой науке и попытался ее опубликовать. Сделать это было непросто: в 1952 году «Литературная газета» напечатала [179] материал, в котором кибернетику называли «наукой мракобесов» и «модной лжетеорией»; в другой публикации и вовсе сообщалось, что «поджигатели новой мировой войны используют кибернетику в своих грязных практических делах для разработки новых приемов массового истребления людей — электронного, автоматического оружия».

Впрочем, все это не помешало Китову в том же 1952 году организовать в артиллерийской академии отдел вычислительных машин. К концу 1950-х он превратился в первый советский вычислительный центр (ВЦ-1, сейчас — центральное НИИ-27 Минобороны); специально для него построили здание на Хорошевском проезде — неподалеку от других военных НИИ Минобороны и главного здания ГРУ.

Именно в ВЦ-1 рассчитывали орбиты первого в мире искусственного спутника Земли, который СССР запустил в космос в 1957 году. В подчинении у Китова было больше тысячи человек, но набирать их было особо неоткуда: специальности «кибернетика» в советских вузах не было. Тогда ученый решил брать студентов технических вузов, которые были способны написать простейшую программу, и переучивать для военной службы — фактически так же в последние годы действует российское Минобороны, привлекая выпускников тех же технических вузов в «научные роты».

«Мы уже привыкли как к режиму секретности, так и к тому, что наши судьбы решаются где-то и кем-то, — вспоминал [180] один из студентов «спецнабора». — И так как это нужно было государству, то мы ожидали своей участи достаточно спокойно».

Другой студент рассказывал [181], как его однажды вызвали к начальнику курса технического университета, в котором он учился:

– На основании ваших хороших учебных результатов подполковник Китов отобрал вас предварительно для работы в создаваемом им вычислительном центре минобороны СССР, чтобы работать на каких-то вычислительных машинах, – сказал начальник курса.

– А что это такое? Я об этом ничего не знаю.

– Во всем министерстве обороны в вычислительных машинах никто, кроме Китова, ничего не понимает. Не робейте. Вы человек неглупый – разберетесь.

На встрече с новичками Китов объяснял, что им предстоит стать «пионерами» создаваемой в Вооруженных силах организации по разработке ЭВМ. Работа в ВЦ-1 больше была похожа на продол-



жение учебы: после рабочего дня или во время него Китов читал лекции «Программирование для ЭВМ», «Теория автоматического регулирования», «Теория множеств». Большую часть времени сотрудники занимались программированием, пытались писать код, делая его как можно короче. Именно в ВЦ-1 разрабатывались первые информационные системы для ГРУ.

Китов стал основоположником советской военной информатики. Он постоянно выступал в секретных НИИ и публиковался в военных журналах. Переработанные материалы в итоге стали двумя книгами — «Электронные цифровые машины» и «Элементы программирования»; после этого издательство «Знание» выпустило упрощенную версию его работ для массового читателя.

В одной из книг Китов развивал свою новую идею — создать сеть ЭВМ для управления страной, фактически первую в мире государственную сеть, прообраз интернета. Свой проект ученый назвал «Красная книга». В январе 1959 года он отправил несколько писем тогдашнему генсеку Никите Хрущеву, подробно изложив свою концепцию. Китов считал, что создание «Красной книги» позволит СССР обогнать Америку в области вычислительных машин, а сама сеть сможет решать как хозяйственные, так и оборонные задачи.

«Наличие единой сети информационных и вычислительных машин позволит также быстро и оперативно собирать и обрабатывать необходимые статистические сведения о состоянии отдельных предприятий, наличии материалов, денежных средств, рабочей силы и т. д. и оперативно использовать результаты обработки для планирования и руководства хозяйством», — писал Китов. Ученый предлагал создать бункеры, в которых будут располагаться вычислительные центры; руководить ими должны были военные. Один из учеников Китова позже говорил, что на реализацию «Красной книги» понадобилось бы больше ресурсов, чем на атомный и космические проекты вместе взятые.

До Хрущева письма не дошло. Его сын вспоминал [\[182\]](#), что идея не понравилась идеологическому отделу ЦК. Суслов «начал на-шептывать», что из-за «Красной книги» «роль партии в сельском хозяйстве сведется к нулю».

Комиссия Министерства обороны СССР сообщила сотрудникам, что «усмотрела в предложениях Китова не государственный, а какой-то личный, карьерный интерес», и обвинила ученого в попытке опорочить руководство Минобороны и принизить руководящую роль КПСС. Китова исключили из партии и уволили, запретив занимать руководящие должности. Его перевели в НИИ-5, где он занялся созданием программного обеспечения для военных. Вскоре он познакомился с Виктором Глушковым, математиком, который от корки до корки прочитал книги Китова. Вместе они продолжили разрабатывать идею создания сети советских ЭВМ. Вскоре они узнали, что государство решило вложиться в создание нескольких вычислительных машин, полностью скопированных с американских IBM-360.



Утром 6 сентября 1960 года на Суворовском бульваре (сейчас — Никитский бульвар) в центре Москвы было необычайно многолюдно. Возле трехэтажного особняка стояли десятки журналистов, рядом — еще больше непримечательных мужчин, вглядывающихся в толпу. Ближе к 11 утра все они собрались в зале Центрального дома журналиста. На сцену поднялись и сели за стол два человека в костюмах; их представили как сотрудников американского Агентства национальной безопасности, которые приехали в СССР, чтобы получить политическое убежище. Это было первое появление Уильяма Мартина и Бернона Митчелла на публике.

С собой мужчины принесли несколько листов бумаги с заявлением. Мартин зачитал его перед собравшимися:

Мы хотим объяснить нашим родным, друзьям и другим лицам, которые могут этим интересоваться, мотивы, побудившие нас просить гражданства Советского Союза. С начала работы в Национальном агентстве безопасности, с лета 1957 года, мы убедились в том, что правительство Соединенных Штатов сознательно делает ложные и вводящие в заблуждение заявления, как для оправдания своей собственной политики, так и для осуждения действий других государств. Нам стало известно, что правительство США давало деньги шифровальщику, работающему в посольстве одной из стран-союзников в Вашингтоне, за информацию, которая помогла расшифровать зашифрованные телеграммы этого союзника. Такие действия убеждают нас в том, что правительство Соединенных Штатов неразборчиво в средствах, хотя оно обвиняет в этом правительство Советского Союза. Многие люди, работающие в Министерстве обороны и в разведывательных организациях правительства США, знают, что наши утверждения являются верными.

Американцы также сказали, что не согласовывали свою речь с советским правительством и считают, что в СССР им будет лучше жить и работать по профессии, ведь в этой стране у женщин больше прав, чем в США, а экономическая и политическая системы служат интересам человека.

Зачитав заявление, Мартин и Митчелл начали рассказывать о том, как устроено АНБ, сколько сотрудников там работают. Они заявили, что агентство «оборудовано тысячами электронно-вычислительных машин для разведки и перехвата сообщений по всему миру». По их словам, американские спецслужбы читали большую часть писем, которые присылали в страну из-за границы.

— Что вам известно о шпионаже СССР в США? — спросил [\[183\]](#) кто-то американцев.

— Насколько мне известно, СССР не осуществляет воздушный шпионаж, как делает США. — ответил Мартин.

— Чем вы сейчас занимаетесь?



— Изучаем русский язык.

В США перебежчиков называли [\[184\]](#) предателями и предложили расстрелять. После того как правительство намекнуло, что один из них, возможно, был геем, в прессе началось обсуждение того, как гомосексуалы угрожают национальной безопасности. Чаще всего журналисты именовали их просто «близкими друзьями-холостяками».

Митчелл и Мартин, родившиеся на рубеже 1920-х и 1930-х, во время Великой депрессии, познакомились в армии: они вместе служили в Японии. В 1957 году, когда оба окончили университет, их завербовали в АНБ — как математиков. Друзья увлекались шахматами, штудировали русские учебники с задачами и посещали шахматный клуб, куда периодически заходил [\[185\]](#) советский дипломат Валентин Иванов. В декабре 1959 года Митчелл и Мартин, готовя побег, летали в Мехико и на Кубу, где встречались с представителями советского посольства. В 1960 году они взяли отпуск, якобы чтобы навестить родителей, и уже не вернулись.

Когда в АНБ хватились сотрудников, отыскать Митчелла и Мартина уже никто не смог. Ведомство начало внутреннее расследование, в рамках которого были допрошены 450 человек, но смогли отследить их перемещения только до Кубы. В доме одного из пропавших нашли ключ, который подошел к сейфу. Внутри лежало «Заявление» — то же самое, которое в сентябре 1960-го Мартин прочтет в Москве. Никаких связей с советскими шпионами расследователи так и не нашли и сочли, что причина их побега — персональные «аномалии»: в АНБ считали их эгоистами, социопатами, атеистами; в секретном архиве особенно подчеркивается, что соседи подозревали их в гомосексуальности.

В СССР американцы сменили имена и начали [\[186\]](#) работать в НИИ, связанных с математикой и криптографией. Источник АНБ сообщал, что Мартин — теперь его звали Владислав Соколовский — стал «неизлечимым алкоголиком, окруженным вырожденками, и практиковал сексуальные извращения».

В мае 1965 года прочитать лекцию в ЛЭТИ (Ленинградский электротехнический институт; позже он выпустит десятки специалистов по кибербезопасности) приехал Клод Шэннон — один из основных американских криптоаналитиков и математиков, придумавший называть наименьшую единицу информации битом. После выступления к нему подошел Бернон Митчелл.

Представившись, Митчелл признался, что теперь работает в советском аналоге ФБР (вероятно, КГБ), а Шэннону просто хотел задать несколько вопросов по теме лекции. По ним Шэннон понял, что Митчелл занимается криптографией; в конце разговора Митчелл признался, что помогает СССР в информационной войне с США.

В конце 1970-х Мартин устал от советской жизни и начал проситься обратно домой, но американцы ответили на его запрос отказом и лишили гражданства; он умер в Мексике в конце 1980-х. Митчелл оставался в России до конца своих дней и даже женился на



преподавательнице фортепиано из Ленинграда; он умер в Петербурге в 2001 году и похоронен там же.

Как рассказывали сотрудники спецслужб, именно информация, полученная от двух перебежчиков из АНБ, подтолкнула советские власти к тому, чтобы снова всерьез заняться криптографией и информационной безопасностью.

\*\*\*

В 1960-х ученик Анатолия Китова Виктор Глушков возглавил Институт кибернетики в Киеве. В команду он набрал молодых амбициозных ученых; вместе они работали над развитием проекта Китова о распределенной сети компьютеров — то, что раньше называлось «Красная книга», теперь бюрократически именовалось «Общегосударственная автоматизированная система учета и обработки информации» (ОГАС).

Как и в любом советском НИИ, в институте, где велись исследования, связанные с ОГАС, много занимались далекими от работы делами, например, придумали называть институт страной Кибертонией и разработали для нее свою конституцию и валюту из перфокарт. Правил выдуманным государством якобы совет роботов, который возглавлял робот-саксофонист; ученые издавали газету «Вечерний Кибер» и проводили кибертонические конференции.

По задумке Глушкова ОГАС должна была упорядочить и ускорить принятие решений для советской плановой экономики. Главный вычислительный центр должен был находиться в Москве; он соединялся с 200 вычислительными центрами поменьше, расположенными в регионах, а они — по телефонным линиям — со всеми заводами и предприятиями в стране, сотрудники которых могли напрямую контактировать друг с другом.

1 октября 1970 года Виктор Глушков отправился в Кремль на решающую встречу с Политбюро. На заседании решили, что проект требует слишком много денег, а запускать его слишком рано: советские чиновники во второй раз отказались от попытки создать компьютерную сеть. В США в те же годы уже вовсю создавали предшественницу интернета, сеть ARPANET.

В 1970 году Глушков вместе с женой Галиной (друзья звали ее «матерью кибернетики») поселился в «Доме на набережной» почти напротив Кремля. Ученый читал лекции о кибернетике в технических вузах, а в 1971 году даже съездил в командировку в Вашингтон, откуда спрашивал у жены, какое она хочет пальто. «Замшевое с норковым воротником или лучше из синтетики? Володе [сын] и себе, может, тоже по демисезонному пальто, — писал супруге Глушков. — Сейчас вечер, сижу в гостинице, буду разбирать технические материалы, полученные днем, посмотрю телевизор и спать».

В 1980 году сын Анатолия Китова Владимир женился на дочери Глушкова Ольге — так две семьи главных советских кибернетиков породнились. В 1985 году, когда генсеком избрали молодого Михаи-



ла Горбачева, Глушков снова предложил властям свою систему. Ему ответили: «У Политбюро ЦК КПСС есть другие функции, а не занятие автоматизацией управления народным хозяйством». После этого большую часть времени ученый проводил на даче. Умер он в 2005 году.



## Глава 27

### «Квант» и «Галилей»

Военные НИИ, созданные во многом на основе идей Китова и Глушкова, теперь стали местами, где формируются российские кибервойска. В научные роты людей ищут по тем же принципам, по каким когда-то набирал сотрудников Китов. В ЦНИИ-27 — так теперь называется бывший Вычислительный центр-1 — сейчас производят средства информационной защиты. Там же находится главный для Минобороны центр аттестации новых программ. В него постоянно ищут научных сотрудников для разработки военных информационных технологий с предполагаемым окладом в 10-20 тысяч рублей. Частью ЦНИИ-27 несколько лет был ЦНИИ-16 Минобороны, в котором занимаются [\[187\]](#) исследованием безопасности сетей связи.

В ЦНИИ-27 и подобных ему институтах теперь часто нанимают хакеров. Несколько человек, которых звали на работу в подобные организации, рассказали мне, что обычно там работают неплохие специалисты. Особенно они выделили несколько институтов: НИИ «Квант», воинская часть 26165, воинская часть 74455, научно-практический центр «Атлас», научно-инженерное предприятие ФСБ № 1, НИИ «Эшелон» и другие. Институтов, в которых занимаются информационной безопасностью, десятки, в них работают тысячи людей, которые обычно при устройстве на работу подписывают соглашение о доступе к секретной информации.

На задворках московского района Ховрино стоит пятиэтажное здание из грязного серого кирпича без опознавательных знаков. Вокруг — забор с колючей проволокой; окна первых этажей покрашены белой краской, некоторые заклеены фиолетовой пленкой. Рядом — промзона и железнодорожные пути, и случайные прохожие здесь не появляются.

В здании находится НИИ «Квант». Он появился в 1978 году на базе конструкторского бюро промышленной автоматики, которое создавало первые советские ЭВМ. Сейчас «Квант» считается базовым научным центром по созданию компьютерных систем специального назначения и систем защиты информации. «Направления работ института имеют государственную значимость», — указано [\[188\]](#) на сайте НИИ. Несколько человек, занимающихся кибербезопасностью в России, сказали мне, что в «Кванте» занимаются исследованиями кибероружия. Один из российских хакеров рассказывал, что туда зовут на работу неболтливых выпускников факультетов информационной безопасности.

В 2008 году «Квант» перешел [\[189\]](#) в ведение ФСБ. К тому моменту в нем уже третий год заместителем директора работал выходец из спецслужб Георгий Бабакин: в 1998 году он окончил институт криптографии академии ФСБ, а до 2005 года работал в силовых ведомствах.

1 апреля 2011 года Бабакину пришло [\[190\]](#) деликатное письмо из Италии. Ему писал Марко Беттини, сотрудник компании *Hacking*



*Team*. К письму он приложил несколько файлов: руководство по использованию программы-вируса *Remote Control System*, ее демоверсию и ссылки на скачивание.

*Remote Control System* (еще программу называли «Галилей») позволяла отслеживать все действия на зараженном устройстве: делать снимки экрана, подключаться к веб-камере и микрофону, перехватывать переписку в мессенджерах и электронной почте, распознавать, какие клавиши нажимал обладатель компьютера или смартфона. Все эти данные собирались в анкету цели — владелец RCS мог просматривать их в удобном интерфейсе. Программа продавалась и продается [191] легально за сотни тысяч долларов, ее покупали в большинстве стран мира (от Нигерии и Уганды до США и Италии) «для улучшения борьбы с преступностью».

4 апреля Беттини отправил россиянину еще одно письмо: «Попробовали демо? Как оно? Сообщите, как будете готовы к заражению. Как думаете, кому мне отправить расценки, вам или „Инфотекс“?» (Российский разработчик защищенных программ для спецслужб и Минобороны. — Прим. Авт.).

Бабакин тут же ответил: «Скачал, спасибо. Мы сейчас вместе с „Инфотексом“ работаем над установкой демо и подсоединением к вашему серверу. Расценки можете отправить и мне, и „Инфотексу“, мы партнеры. Правда, думаю, они не используют PGP [\*\*\*], так что я им все перешлю:»).

5 апреля Бабакин снова написал Беттини. «Как у вас со временем для презентации в мае в Москве?» — спросил он итальянца.

По всей видимости, речь шла о презентации программы для ФСБ. В другой переписке [192] указано, что через месяц после этого диалога RCS в Москве продемонстрировали двум разным группам сотрудников силового ведомства. Им показывали, как программа может отслеживать зараженные ноутбуки. «Реакция [ФСБ] была крайне положительной, нам задали много вопросов о возможностях. Из их вопросов стало понятно, что у них есть опыт легальных взломов, но, видимо, у них нет возможности заражать мобильные устройства и Mac», — отмечали в переписке представители *Hacking Team*.

В 2012-2014 годах «Инфотекс», представляя НИИ «Квант», выплатил [193] итальянской компании 451 тысячу евро. Позже компания заявила [194], что приобрела RCS для «повышения уровня экспертизы компании в области практической информационной безопасности».

«Государственные компании и органы, которые покупали что-то у *Hacking Team*, покупали это для слежки, — утверждает специалист одной из ведущих российских компаний по кибербезопасности. — Уязвимости покупают не для защиты инфраструктуры, а для активных мероприятий».

В 2013 году Георгий Бабакин ушел из «Кванта» на должность руководителя проектов в департамент информационной безопасности МТС. Это мне подтвердил представитель мобильного оператора



Дмитрий Солодовников. Российские оппозиционеры настаивают, что МТС сотрудничает со спецслужбами. В апреле 2016 года российский оппозиционер Олег Козловский и сотрудник Фонда борьбы с коррупцией Георгий Албуров обвинили [\[195\]](#) МТС в участии во взломе их аккаунтов в *Telegram*: неизвестным тогда удалось перехватить авторизационные коды от аккаунтов жертв взлома, которые должны были прийти им по SMS (но не пришли). Козловский позже рассказал, что МТС в момент взлома отключил службу доставки SMS. В службе поддержки ему заявили, что сделал это отдел технической безопасности компании. Позже активисты выложили квитанции за услуги за апрель 2016 года: и у Козловского, и Албурава в них указано отключение услуг коротких сообщений.

\*\*\*

Деятельность российских военных НИИ, в которых занимаются разработкой и исследованиями информационной безопасности, почти всегда засекречена. Их сотрудники находятся под подпиской о неразглашении и к тому же зачастую боятся преследований со стороны государства. Даже родители погибших на Украине российских военных в основном отказывались общаться с журналистами. Я ездил к нескольким, находил могилы их сыновей с венками от Минобороны, но их родственники меня выгоняли и просили больше никогда не появляться. Уголовные дела о разглашении гостайны в последние годы в России заводятся все чаще — и по самым безобидным поводам. Например, в январе 2015 года в госизмене обвинили [\[196\]](#) жительницу Вязьмы Светлану Давыдову: по мнению ФСБ, в апреле 2014 года Давыдова позвонила в посольство Украины в Москве, чтобы сообщить о том, что на Украину направляются солдаты расположенной рядом с ее домом воинской части. Давыдова отсидела два месяца в СИЗО «Лефортово», после чего уголовное дело закрыли, видимо, из-за общественного внимания.

О том, что происходит в военных институтах и чем они занимаются, приходится узнавать из редких новостей. В 2012 году сотрудники НИИ ФСБ № 1, находящегося в подмосковном городе Железнодорожном, пытались [\[197\]](#) незаконно купить микроэлектронику в США — для изучения шифрования. Ранее тот же институт исследовал «антропоморфные методы анализа и обработки речи», «способы автоматического распознавания личности по голосу», «способы изменения и имитации голоса заданной личности».

Иногда о своих исследованиях военные ученые рассказывают сами. В одном из отчетов [\[198\]](#) НИИ «Эшелон» за 2013 год подробно говорится о поисках уязвимостей в зарубежных программах; указано, что «иногда обнаруживаются закладки в продукции (программах и устройствах. — Прим. Авт.)», а «один из способов противодействия подобным угрозам — проверка безопасности программного кода в процессе сертификационных испытаний».



жит [\[201\]](#) квартира в одном доме с ближайшим окружением Владимира Путина.

На одну из профильных конференций «Параллельные вычислительные технологии» в Архангельске Георгий Рошка ездил вместе с Сергеем Зайцевым, сотрудником Центра специальных разработок Минобороны. Помимо них на конференцию приезжали сотрудники того же «Кванта» и военнослужащие частей, занимающихся электронной разведкой. Сам Рошка в программе конференции был указан как специалист войсковой части 26165 — за этими цифрами скрывается 85-й главный центр специальной службы Генштаба, который располагается на Комсомольском проспекте в Москве, в историческом здании Хамовнических казарм, построенном в начале XIX века. Военной частью долгие годы руководил генерал Сергей Гизунов, хорошо разбирающийся в криптографии. Последние годы он работает заместителем начальника ГРУ; в 2016 году США внесли его в санкционные списки по подозрению в участии в хакерских атаках.

Именно из зданий Хамовнических казарм уезжал на такси в аэропорт Алексей Моренец, которого в 2018 году обвинили [\[202\]](#) в попытке атаки на Организацию по запрещению химического оружия в Нидерландах. Там же, на Комсомольском проспекте, по версии американских прокуроров, работали [\[203\]](#) 10 хакеров и сотрудников ГРУ, которые, как считает американская разведка, атаковали сервера Национального комитета Демократической партии США.



По словам моего собеседника, специализирующегося на безопасности государственных объектов, подобные занятия не имеют смысла. «Идея в том, чтобы злые американцы нам не прислали оборудование с закладками. Оборудование якобы проверяют и перепродают [госкомпаниям]. Это на ровном месте накрутка денег, потому что реально проверить их невозможно, — объясняет источник. — К тому же они продают их без поддержки или с задержкой обновлений. И стоят такие компы в закрытых режимных комнатах, но напроць дырявые».

«В НИИ работают прошаренные люди — это можно понять, например, из истории про „Квант“. Во многих НИИ есть дорогостоящие программы официально „для тестирования на проникновение“, а на самом деле для взломов, — продолжает собеседник. — Это графический интерфейс с кучей эксплойтов. Обычно такие вещи покупаются для ФСБ. Такие штуки стоят тысячи долларов в год, но в НИИ ими будто не пользуются. Их держат для интереса спецслужб — они нужны для понимания, какими могут быть атаки».

Хакер рассказывает эту историю, когда мы бродим кругами по большой автомобильной развязке — там шумно, легко потеряться и безлюдно: любую слежку сразу будет заметно.

По его словам, многих программистов на рынке зовут на работу в НИИ, «связанные с конторой». Одному из пришедших на собеседование на такую работу намекнули на найденные уязвимости нулевого дня в одной из самых распространенных программ.

\*\*\*

5 мая 2017 года, за день до президентских выборов во Франции, *Wikileaks* выложил архив взломанных переписок Эммануэля Макрона и его штаба. На выборах ему противостояла Марин Ле Пен из «Национального фронта». В разгар кампании она встречалась с президентом России Владимиром Путиным, ее не раз обвиняли в тесных связях с РФ. Ситуация будто бы повторяла осенние события 2016 года в США: там во время президентской кампании хакеры взламывали почту соратников Хиллари Клинтон, пока Путин и кандидат от республиканцев Дональд Трамп обменивались комплиментами.

В 9 гигабайтах почты Макрона находилась переписка членов партии и сотрудников его предвыборного штаба, а также некоторые финансовые документы. В одном из писем указывалось, что Макрон серьезно болен. При этом почти сразу выяснилось [\[199\]](#), что девять файлов были изменены неким пользователем по имени Георгий Петрович Рошка.

Программист Георгий Петрович Рошка оказался [\[200\]](#) сотрудником ЗАО «Эврика». «Эврика» занималась производством программного обеспечения для Минобороны и спецслужб, в частности, выполняла заказы для НИИ «Квант». Совладельцу «Эврики» принадле-



## Глава 28

### Солдаты криптографии

Большинство руководителей российских компьютерных компаний и спецслужб — ГРУ, ЦИБ ФСБ, отдела «К» Министерства внутренних дел — учились в институте криптографии, связи и информатики академии ФСБ (до 1991 года — 4-й технический факультет высшей школы КГБ). В 1987 году ее окончил создатель «Лаборатории Касперского» Евгений Касперский — он получил специальность «инженер-математик». Там же учился Георгий Бабакин, впоследствии возглавивший НИИ «Квант». Выпускниками академии оказались и несколько действующих хакеров, с которыми я встречался, собирая материал для этой книги.

Михаил Масленников, один из выпускников высшей школы КГБ, говорил [\[204\]](#), что обучение было похоже на «Уловку-22» (крылатое выражение, обозначающее абсурдные взаимоисключающие требования, произошедшее от одноименного антивоенного романа Джозефа Хеллера. — Прим. Авт.). 4-й факультет, специализировавшийся на криптографии, находился в особняке в Большом Кисельном переулке на Лубянке (сейчас академия переехала в модернистское здание на Мичуринском проспекте). Перед входом в актовый зал висел плакат «*You are welcome*». Преподаватели следили за внешностью и прическами студентов; на строевой подготовке часто звучали фразы вроде «Стоящий рядом товарищ подчеркивает вашу неподстриженность», «В строю должно быть однообразие, именно этим он отличается от бесстроия». К математикам-криптографам относились, как к обычным солдатам, у которых в первую очередь должны быть чистыми сапоги, а коды и формулы — это уже потом.

На лекциях по матанализу студентам рассказывали о том, что действовать нужно последовательно — небольшими шагами (как и в программировании, где строки кода постепенно соединяются в большую программу). Иногда математиков отправляли работать в «поле» как обычных агентов: они внедрялись в толпу на массовых мероприятиях, чтобы предугадывать «возможные инциденты». Когда 8 января 1977 года в Москве произошли несколько терактов (семь человек погибли, около 30 ранены; в преступлениях обвинили «Национальную объединенную партию Армении»), у студентов отменили новогодние каникулы; им пришлось сутками кататься на метро, где произошел один из взрывов, чтобы «предотвращать теракты».

Во время учебы им часто рассказывали об успешных операциях по дешифровке, в которых спецслужбы СССР во многом ориентировались на американское АНБ. В свободное от лекций время многие студенты уходили в дальние углы библиотеки, предназначенные для работы с секретными документами, чтобы поиграть в преферанс — его любили за математичность, возможность подсчитывать варианты.



После выпуска из высшей школы КГБ Масленникова направили на работу в 8-е управление КГБ — советский аналог Агентства национальной безопасности. Ему назначили зарплату в 250 рублей — в два раза больше, чем у начинающего сотрудника любого НИИ. В управлении постоянно говорили о сверхзадаче создания новой шифровальной аппаратуры.

Работа начиналась в 9 утра, но уже через два часа объявлялась «пятиминутка физкультуры» — на ней играли в шахматы. Вскоре приходило время обеда; дальше — ожидание конца рабочего дня. Все это не слишком отличалось от других советских институтов. «Там часами не вылезали из курилок, травили анекдот за анекдотом, обсуждали всё что угодно: хоккей, очередной фильм по телевизору, институтские сплетни, где что достать (свободно купить что-то приличное в те годы было невозможно), вязали носки и свитера, бегали по магазинам, — вспоминал выпускник высшей школы КГБ. — Работы как таковой почти нигде не было, везде правили серость и скука, порождающие равнодушие и пьянство». Иногда математиков отрывали от разработки шифров для слежки за иностранными туристами — так было во время московской Олимпиады-80.

Как вспоминает Масленников, 8-е управление КГБ почти перестало работать, когда у них появились компьютеры, на которые можно было установить видеоигры. Больше всего их занимала *Space Quest 2* — одна из первых «бродилок» про уборщика, попадающего на разные планеты; в обсуждении, как пройти через болото с монстром, проходили целые рабочие дни. Криптографы рисовали схемы прохождения уровней и ругались между собой. Только спустя неделю они заметили, что босса можно пройти, спрятавшись в кусты и съев с них ягоды.

Когда 19 августа 1991 года Государственный комитет по чрезвычайному положению взял на себя власть в стране, всех сотрудников КГБ перевели на усиленный режим службы. Вскоре им сообщили о том, что КГБ поддержит ГКЧП, — но путч потерпел поражение, руководство ведомства арестовали, а в КГБ начались массовые увольнения. Ушел и Масленников. По его словам, многие криптографические алгоритмы и другие разработки управления, в котором он работал, были потеряны; их никто не запатентовал.

Тем не менее криптографический институт при спецслужбе продолжал работать — уже в структуре созданной в 1992 академии Министерства безопасности России (теперь — академия ФСБ). Один из ее выпускников рассказывал мне, что в начале 1990-х он учился в обычной школе на юге Москвы. Туда периодически приходили сотрудники спецслужбы, предлагая поступить в академию. Как-то они пришли вместо урока физики. Двое мужчин пообещали после выпуска не только стабильную работу, но и много приключений. Юноша задумался и решил на следующей встрече узнать подробности. Она состоялась только через год; обсудив математические успехи школьника, силовики предложили ему поступать в институт криптографии академии.



Он сдал два экзамена по математике — письменный и устный, физику, написал сочинение и набрал проходной балл. После проверки всех родственников его зачислили в академию. Порядки там оказались военные: жесткий распорядок дня, курсы по стрельбе (при этом больше половины времени отнимали [\[205\]](#) лекции и семинары по математике). В начале 1990-х в вузе чувствовался такой же упадок, как и во всем российском государстве. Один из преподавателей вспоминал позднесоветские времена, когда в институте работали лучшие математики и криптографы. Другой рассказывал, что курсы по криптографии и дешифровке основывались в том числе на работах, полученных от перебежчиков АНБ.

Чтобы искать новых потенциальных студентов, с 1991 года ФСБ начала проводить олимпиады по криптографии среди школьников. Юных хакеров в спецслужбе ищут и сейчас.



## Глава 29

### Юные программисты ФСБ

В 2015 году в Московском кадетском корпусе, который располагается недалеко от метро «Коломенская» на юге Москвы, появился кружок «Юные программисты ФСБ России».

В нем занимаются школьники 9-11 классов. Кружок организовал учитель информатики Сергей Епифанцев. Он рассказывал, что проект создан для того, чтобы «противостоять всяким „укропам“ (то есть украинцам. — Прим. Авт.), быдлу, всем тем, кто поддерживает американский образ жизни, противостоять „пятой колонне“, врагам современной России», а его ученики будут «стоять у истоков новой российской IT-индустрии, свободной, по выражению нашего президента, от иностранного программного обеспечения». Епифанцев писал [206], что занимается «подготовкой будущих специалистов в области информационных технологий для силовых структур».

Епифанцев создал кружок при участии пограничного музея ФСБ России и Центрального музея вооруженных сил — для них в 2015 году ученики создавали программное обеспечение. Заместитель директора ЦМВС полковник Владимир Афанасьев подтверждал [207], что они поддерживают проект.

В подробной презентации [208], размещенной на сайте кадетского корпуса, рассказывалось, что «юные программисты» в рамках курсов по основам информационной безопасности изучают, как устанавливать и использовать уязвимое программное обеспечение, как делаются DDoS-атаки. Также они занимаются перебором паролей к почтовым ящикам, уязвимостями публичного вайфая (на примере вайфая в московском метро) и радиоперехватами телефонных переговоров (в том числе с помощью дронов). Эти исследования они с февраля 2017 года проводят совместно с кафедрой компьютерных систем и технологий МИФИ.

В конце декабря 2016 года «юные программисты» участвовали [209] в конкурсе *Moscow School CTF*, на который пришли [210] в военной форме. Они заняли четвертое место. Хакер и постоянный участник CTF сказал мне, что такие мероприятия — главное место, где специалистам по информационной безопасности предлагают работу в спецслужбах: к хакерам подходят в перерывах, раздают буклеты, зовут приехать поговорить.

Соревнования, в которых участвовали «юные программисты», проводились при поддержке Центра специальных разработок Минобороны, куда, по словам моих собеседников, чаще всего зовут на работу специалистов по информационной безопасности. Минобороны создало ЦСР в 2014 году, сотрудников в него искали среди выпускников технических вузов; в вакансиях указывалось, что больше других в ЦСР Минобороны нужны сотрудники для анализа эксплойтов (программ для проведения компьютерных атак) и «реверс-инжиниринга» (исследования механизмов работы программ и устройств для их последующего воспроизведения). Хакер, которого



звали на работу в ЦСР, рассказал, что уговорить пойти работать в спецслужбы удастся немногих хакеров и специалистов из коммерческих компаний, потому что они часто не хотят, чтобы им ограничивали выезд за границу.

На сайте кадетского корпуса указано [\[211\]](#), что после соревнований в декабре 2016 года «юные программисты» в неформальной обстановке пообщались с сотрудниками ФСБ, которые «высоко оценили подготовку обучающихся» и «признали [их] перспективными для повышения обороноспособности нашей страны от киберпреступлений и кибератак».

Для рассказа о деятельности проекта Епифанцев зарегистрировал сайт с доменом [fsb.ru.com](#). На главной странице была размещена его фотография [\[212\]](#) на фоне герба ФСБ; там же была опубликована ссылка [\[213\]](#) на презентацию проекта, в которой рассказывалось о сотрудничестве с Минобороны и ФСБ.

В конце января 2016 года «юным программистам» прочитал лекцию [\[214\]](#) о современных войнах сотрудник ФСБ Олег Кржижановский. «Война уже идет! — заявил он сразу. — Как минимум на двух фронтах, потому что на Украине и в Сирии участвуют наши военнослужащие». После этого рассказал школьникам, что «если изолировать 30 самых могущественных евреев, то войны прекратятся», а большинством процессов в мире управляют корпорации вроде *General Motors, Shell, Coca-Cola, McDonald's*. «Что вообще такое война? У нас срабатывает стереотип: танки, пехота, штыковая атака, окопы. Но войны сплошным фронтом больше не будет. Сейчас в оборот входит термин „гибридная война“. Это что, как вы думаете?» — спросил Кржижановский. «Это кибернетическая война с помощью интернета. Можно взламывать сайты другого государства, смотреть информацию оттуда, использовать ее против них», — сказал один из «юных программистов». «Правильно!» — сказал преподаватель. «Еще — когда подменяют идеи с помощью СМИ, — предложил другой школьник. — Или когда с помощью митингов, которые устраивают шпионы, подводят народ, чтобы он свергнул свое правительство». «Правильно, добавим сюда еще теракты как средство расшатывания общества, — сказал Кржижановский. — Также есть целая методичка по ненасильственному сопротивлению».

Кржижановский, работающий в музее ФСБ и защитивший [\[215\]](#) диссертацию по теме «Формирование мотивации к военной службе у юношей допризывного возраста в процессе социально-культурной деятельности военно-исторического музея», рассказал школьникам про «оранжевые революции» и то, как «разыгралась трагедия в Ливии, когда убили законного лидера Муаммара Каддафи». «Почему же тогда бы нам всем не объединиться и не напасть на Америку?» — спросил один из учеников.

Помимо встреч в музее, школьники посещают [\[216\]](#) соревнования с активистами «Молодой гвардии „Единой России“» и выступления [\[217\]](#) главы Следственного комитета Александра Бастрыкина; фотографируются [\[218\]](#) с портретом Владимира Путина. Также они



переводили [\[219\]](#) книгу про американского хакера, который воровал данные кредитных карт и разоблачал педофилов (школьники прозвали его «хакером-тесаком», видимо, имея в виду основателя движения «Оккупай-педофилия» Максима «Тесака» Марцинкевича); в книге, помимо прочего, подробно рассказывается про работу спецслужб в сфере информационной безопасности. За свои достижения «юные программисты» получают [\[220\]](#) десятки грамот — один из учеников в августе 2015 года удостоился [\[221\]](#) нагрудного знака «95 лет ВЧК-КГБ-ФСБ».

«Юные программисты» учатся в музыкальном кадетском корпусе, поэтому периодически записывают видеоклипы — весной 2017 года они сняли [\[222\]](#) «Гимн российской сборной к чемпионату мира по футболу 2018 года», который представляли [\[223\]](#) на базе ЦСКА. Есть у учеников и ролики против экстремизма. Один из них заканчивается [\[224\]](#) кадром, на котором «юные программисты» и Епифанцев в шутку вскидывают руки в нацистском приветствии — эта картинка снабжена надписью «Правда это смешно?»

Рассказывать о своей работе Епифанцев отказался. «Я не желаю с вами разговаривать», — сказал он. Епифанцеву 37 лет, он окончил Московский государственный областной гуманитарный институт по специальности «информатика». До кадетского корпуса он работал [\[225\]](#) заместителем директора специального интерната в Ногинске и руководил военно-патриотическим клубом «Факел», за работу в котором получал благодарность от Голицынского пограничного института ФСБ. На сайте департамента образования Москвы указано [\[226\]](#), что Епифанцев — ветеран боевых действий, у него есть медаль «25 лет вывода советских войск из Афганистана» и знак «95 лет оперативно-поисковому управлению ФСБ России».

Я попытался связаться с десятью «юными программистами» в соцсетях. Большинство из них увидели сообщения, но не стали отвечать. Один из учеников сначала согласился на интервью, но потом также перестал отвечать на сообщения. После того как я начал связываться со школьниками, Епифанцев написал мне еще одно сообщение: «Вы всем подряд будете навязывать свое интервью? На каком основании вы спрашиваете детей? Я прошу оставить нас в покое».

25 мая 2017 года кружок «юных программистов» подписал договор о взаимодействии с Академией ФСБ России и управлением ФСБ по Москве.



# Часть IV

## Война

### Глава 30

#### Модный медведь

Холодная кибервойна между Россией и США продолжается с момента, когда закончилась холодная война, — и если в конце 1980-х советские спецслужбы получали секретные американские данные от немецких хакеров, то через несколько лет заниматься взломами начали уже сами россияне.

В 1996 году группировка *Moonlight Maze*, которую связывали с российской разведкой, похитила значительное количество документов из правительственных и университетских сетей США, включая Пентагон и NASA. К расследованию атак подключился Роберт Гурли, опытный сотрудник спецслужб, который во время холодной войны отслеживал советские подводные лодки. Когда его команда исследовала следы кибершпионов, выяснилось, что тех интересуют гидродинамика, океанография, геофизика и технологии слежки и что в хакерском коде были фрагменты на кириллице [227].

Информация об атаке скоро появилась в прессе. В еженедельнике *Newsweek* вышел [228] материал «Мы находимся на кибервойне». В статье говорилось, что публика впервые узнала о попытках российской разведки получить американские технологии — при этом в Минобороны США журналистам заявили, что это «кибервойна уже в разгаре». Военные чиновники называли хакеров «терпеливыми и настойчивыми» и предполагали, что после первого вторжения они просто начали применять новые инструменты: «Зарылись в сети так глубоко, что их невозможно теперь отследить».

В конце концов Белый дом одобрил запрос ФБР на поездку в Россию для встречи с представителями спецслужб. Американцы решили не обсуждать взломы как дело государственной важности, а просто попросить помощи коллег в расследовании кражи. В Москву отправились около 10 сотрудников спецслужб США.

Их встретили как дорогих гостей — весь первый день визита представлял собой сплошное застолье с тостами, водкой и икрой. На следующий день американцы отправились в российское Министерство обороны. Когда он обсуждали атаки, их собеседник, генерал армии, смущенно обвинил «этих ублюдков в разведке» и заявил, что не приветствует подобные действия. Это была последняя встреча американцев с российскими военными — агенты ФБР провели в Москве еще четыре дня, но в Минобороны их больше не звали. На следующие несколько лет хакеры, которых связывали с Россией, замолчали.

Профессор Королевского колледжа Лондона Томас Рид продолжал расследование действий *Moonlight Maze* следующие два десят-



ка лет. В 2016 году оно привело его в одну из английских деревень, в которой жил эксперт по компьютерной безопасности, анализирувавший атаки 1996 года. Рида интересовал один из его компьютеров, который взломали русские хакеры; оказалось, что тот до сих пор его хранит. Лондонский ученый исследовал компьютер вместе с экспертами из «Лаборатории Касперского» и обнаружил часть вредоносного кода того времени. Оказалось, что он до сих пор используется российскими прогосударственными хакерами.

\*\*\*

Атаки российских хакеров на различные американские институты продолжались годами, но самыми резонансными и, видимо, эффективными стали взломы 2015 года. Тогда хакеры из группировки *Fancy Bear* — судя по всему, представители российских кибервойск — внедрились в систему Национального комитета Демократической партии США.

Сделали это они самым простым способом — с помощью фишинговых писем (по данным аналитической компании *CrowdStrike*, демократов взламывали дважды — летом 2015 года и в апреле 2016 года). Получив доступ к переписке высокопоставленных сотрудников комитета и партии, они передали ее *Wikileaks*, которые выложили письма в публичный доступ за несколько месяцев до президентских выборов. В них обнаружилась информация, компрометирующая Хиллари Клинтон, которая баллотировалась на этот пост от демократов: партийные координаторы обсуждали между собой, как насолить ее внутрипартийному конкуренту Берни Сандерсу; одна из представителей партии согласовывала с Клинтон вопросы, которые ей должны были задать во время публичного интервью.

Ответственность за атаку тогда взял на себя хакер *Guccifer 2.0*. Свой псевдоним он позаимствовал у румына Марцела Лехела, который в тот момент находился в американской тюрьме, ожидая приговора за причастность ко взлому почтовых ящиков румынских и американских политиков.

На сайте *Guccifer 2.0* говорилось, что он родом из Восточной Европы и считает, что переписку политиков необходимо предавать огласке. Хакер специально указывал, что не связан с Россией, и отмечал, что все последние хакерские атаки приписывают россиянам, несмотря на то что теми же методами могут действовать люди со всего мира. *Guccifer 2.0* утверждал, что миф о могущественных русских хакерах запустила «Лаборатория Касперского», преследуя собственные бизнес-интересы.

Действия, слова и файлы «Гуччифера» принялись изучать сотни людей — обнаруживая все больше доказательств того, что хакер (или хакеры) все-таки действительно связан с Россией. Одними из самых ярких стали находки в метаданных украденных писем: их открывали на компьютере, использующем русский язык, а одно из



писем исправил [\[229\]](#) пользователь «Феликс Эдмундович»: видимо, хакеры зачем-то оставили таким образом послание.

Когда мне однажды удалось побывать в здании ФСБ, я понял, что Дзержинский по-прежнему остается для сотрудников российских спецслужб героем и символом: календари с его портретом висят чуть ли не в каждом кабинете дома на Лубянке.

С июля 2016 года «российские хакеры» стали одной из главных тем американской политики. Штаб Клинтон сразу же обвинил Кремль в организации атак и помощи Дональду Трампу, кандидату в президенты от республиканцев. Трамп все отрицал; позже, выиграв выборы, он продолжил говорить, что никак не сотрудничал с Россией, — хотя стал допускать, что хакеры могли действовать в интересах Кремля. Пресс-секретарь Владимира Путина Дмитрий Песков заявлял [\[230\]](#), что Россия никаким образом не причастна к атаке.

Расследовать произошедшее начали сразу несколько американских ведомств; в январе 2017 года Управление директора национальной разведки США опубликовало доклад [\[231\]](#), в котором говорилось, что президент России Владимир Путин лично распорядился начать «кампанию по вмешательству» в президентские выборы в США. Такой вывод американская разведка делает «с высокой степенью уверенности».

\*\*\*

Атаки 2016 года, видимо, были частью государственной разведывательной операции, продолжающейся еще с середины 2000-х. В киберзащитной компании *Trend Micro* указывали, что одна и та же группа с середины 2000-х атакует организации и политиков, угрожающие интересам России (во всяком случае, по версии самой России). В 2008 году, например, они атаковали Пентагон. Киберзащитные компании называли российских хакеров по-разному — то *Pawn Storm*, то APT28 [\[\\*\\*\\*\]](#), то *Tsar Team*, то *Fancy Bear*, но их цели оставались примерно одними и теми же. Например, *Fancy Bear* за 2015 год отправили [\[232\]](#) минимум 4400 фишинговых писем — среди адресатов были российские оппозиционеры, политики многих европейских стран, сотрудники НАТО, Демократическая партия США. Рассылали хакеры и письма с зараженными вложениями.

Впервые ответственность за атаку *Fancy Bear* взяли на себя после взлома Всемирного антидопингового агентства — в сентябре 2016 года. Тогда у группы появился сайт *fancybear.net*, оформленный карикатурным медведем в маске движения *Anonymous* — хакеров-активистов, которые в начале 2010-х атаковали террористов, саентологов и правительственные ресурсы, занимающиеся цензурой; там и были выложены [\[233\]](#) документы ВАДА. Взлом произошел через несколько недель после отстранения российских спортсменов от Олимпиады в Рио-де-Жанейро за употребление запрещенных препаратов. Из документов, опубликованных *Fancy Bear*, следовало, что допинг — с разрешения агентства — принимали и известные амери-



канские спортсмены. Представители ВАДА обвинили во взломе Россию.

Прямых доказательств связей между *Fancy Bear* и российскими властями долго не существовало. Среди косвенных свидетельств того, что эти связи существуют, эксперты указывали [234], например, тот факт, что работают хакеры с 9 до 17 часов по московскому времени. В используемом ими коде можно было обнаружить кириллические фрагменты, среди серверов — те, что располагаются [235] в России, а для ответов на запросы журналистов хакеры использовали «российский VPN». Впрочем, главным доказательством все равно остается то, что атаки совершаются фактически в интересах российских властей.

Эксперты киберзащитной компании *Eset* говорили, что группа «отличается высоким уровнем технической подготовки». По их данным, *Fancy Bear* постоянно использует «уязвимости нулевого дня» — ранее неизвестные «дыры» в программном обеспечении (только в 2015 году *Fancy Bear* отыскали их шесть в *Windows*, *Java* и *Adobe Flash*; для сравнения, в кибероружии *Stuxnet*, которое применялось при атаке на иранскую ядерную программу, использовалось [236] четыре уязвимости нулевого дня). Для работы с похожими уязвимостями, видимо, набирали [237] специалистов в Центр специальных разработок Минобороны.

Поиск и разработка таких «дыр» — сложное и долгое дело, а значит, требует серьезных финансовых вложений. При этом группировка не совершала [238] «коммерческих взломов» вроде кражи денег с банковских счетов и не торговала результатами своих исследований (стоимость уязвимостей нулевого дня на черном рынке начинается от нескольких десятков тысяч долларов).

«Лаборатория Касперского» еще в 2014 году рассказывала [239] о группировке АРТ28, действующей теми же методами, что *Fancy Bear*, — до событий с выборами в США эксперты говорили о прогосударственных хакерах значительно свободнее. АРТ28 атаковали Белый дом и Госдепартамент США, используя фишинг и прикрепленные к письмам видеоролики, при открытии которых на компьютер скачивались дополнительные модули вирусов. «Лаборатория Касперского», давно следившая за деятельностью группировки, считала ее участниками россиянами из-за комментариев в коде на кириллице, версий операционных систем, на которых писался код, часовых поясов, а главное, из-за того, что технологии, которые использовали взломщики, пересекались с технологиями других русскоязычных хакерских групп.

\*\*\*

О том, что за взломами серверов Демократической партии стоят не просто российские хакеры, а Минобороны и ГРУ, было официально объявлено в январе 2017 года в [докладе](#), под которым, по сути, подписалось все разведывательное сообщество США. Еще через полто-



ра года последовали подробности — американское жюри присяжных утвердило обвинение в адрес 12 сотрудников Генштаба, осуществлявших атаки. В судебных документах было подробно изложено [240], кто и как, по версии американских исследователей, крал данные у демократов.

Большинство атак курировались из двух зданий — войсковой части 26165 на Комсомольском проспекте (про нее я уже рассказывал) и «башни» в Химках, которая официально называется «Центром управления повседневной деятельностью».

Согласно документам [241] американских спецслужб, подполковник Сергей Моргачёв командовал подразделением воинской части, разрабатывающей хакерское оборудование, в том числе программу *X-Agent*, которую часто используют хакеры. Ему помогали четверо лейтенантов. Борис Антонов руководил группой из четырех человек, которая взламывала компьютеры с помощью фишинговых писем. С ним работали трое сотрудников ГРУ.

Виктор Нетышко (один из сотрудников ГРУ, которым было предъявлено обвинение) оказался кандидатом технических наук, в 2003 году защитившим диссертацию по специальности «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»; в 2010 году он был оппонентом на защите диссертации о компьютерных взломах в РГГУ. Его же подпись стоит под договорами о сотрудничестве между академией ФСБ и рядом московских математических школ — в документах указано, что школьников будут готовить к поступлению в «научные роты» Минобороны. Еще один обвиняемый, Дмитрий Бадин, в 2014 году участвовал в московской хакерской конференции *Positive Hack Days*.

Сотрудники ГРУ атаковали более трехсот компьютеров, связанных с Национальным комитетом Демократической партии США, партийным комитетом по выборам в Конгресс и президентской кампанией Хиллари Клинтон. Они рассылали письма от имени *Google*, якобы содержавшие уведомление о настройках безопасности. Внутри находилась ссылка, которая вела на сайт, созданный ГРУ.

В марте 2016 года таким образом была взломана почта главы избирательного штаба Клинтон Джона Подесты. В его ящике находилось более 50 тысяч писем. После этого сотрудники ГРУ создали почтовый ящик, адрес которого на одну букву отличался от адреса одного из участников кампании Клинтон. С него они разослали фишинговые письма другим сотрудникам штаба. В письмах якобы содержалась ссылка на *xlsx*-документ с рейтингами Клинтон; в действительности она вела на сайт, созданный ГРУ.

Одновременно сотрудники российской разведки атаковали компьютерные системы комитета Демократической партии по выборам в конгресс. Доступ был получен с помощью фишингового письма, отправленного одной из сотрудниц комитета. Она прошла по присланной ей ссылке и ввела пароль. С апреля по июнь 2016 года обвиняемые установили шпионскую программу *X-Agent* по меньшей мере на 10 компьютеров, подключенных к сети партийного комите-



та (этот же модуль устанавливался в Украине в приложениях для расчета баллистики). Программа записывала, какие клавиши нажимал пользователь, и делала снимки экрана его компьютера, а затем передавала украденные данные на сервер, который ГРУ арендовало в Аризоне.

С помощью *X-Agent*, в частности, были похищены пароли сотрудника комитета по выборам в Конгресс, который также имел доступ к сети Национального комитета Демократической партии. Таким образом были взломаны не менее 33 компьютеров, подключенных к этой сети.

На взломанных компьютерах подозреваемые, в частности, искали документы с упоминанием Хиллари Клинтон, Дональда Трампа и участника республиканских президентских праймериз Теда Круза. Они также скачали папки с информацией о расследовании нападения боевиков на посольство США в Бенгази в 2012 году (Хиллари Клинтон в то время занимала пост госсекретаря США, она давала показания по этому делу [\[242\]](#) на слушаниях в Конгрессе). Кроме того, хакеры получили доступ к финансовым документам, в частности, к планам сбора пожертвований на кампанию Клинтон.

Чтобы распространить эти документы, сотрудники ГРУ, по версии американского следствия, притворились румынским хакером *Guccifer 2.0*. Как указано в документе, в июне 2016 года, когда *Guccifer 2.0* обвинили в том, что это имя используется как прикрытие для представителей российских спецслужб, с одного из серверов российской военной части 74455 поступили поисковые запросы о некоторых английских фразах (например, перевод словосочетания «широко известный перевод» или правописание слова *illuminati*). Через два с небольшим часа все эти фразы появились в заявлении *Guccifer 2.0*, в котором «хакер» категорически отрицал связь с Россией.

Тогда же, в июне 2016 года, обвиняемые запустили сайт *DCLeaks*, на котором выкладывали часть украденной переписки. Для его раскрутки были созданы аккаунты в фейсбуке и других соцсетях. Кроме того, они передавали похищенные данные третьей стороне, которая в обвинительном заключении указана как *Organization 1*, — скорее всего, имеются в виду *Wikileaks*.

Несмотря на некоторые доказательства связи российских хакеров из ГРУ с атакой во время президентской кампании в США, вопросов к этой истории не стало меньше. Россия по-прежнему отрицает атаки; ни один из названных сотрудников ГРУ ничего не прокомментировал. Один из моих собеседников — хакер, работавший в ФСБ по международной разведке, — во время одной из долгих прогулок по окраине Москвы рассказывал, что все еще сомневается в способностях ГРУ. Он уверен, что атаки совершали нанятые на форумах хакеры-фрилансеры.



## Глава 31

### «Орки» со товарищи

5 декабря 2016 года — спустя месяц после победы Дональда Трампа на президентских выборах в США — сотрудники ФСБ пришли на совещание к своему коллеге, одному из руководителей Центра информационной безопасности ведомства Сергею Михайлову. Совещание закончилось быстро: Михайлову надели на голову мешок и увели. Его знакомые указывали, что следователи опасались, что Михайлов — обладатель черного пояса по карате — окажет сопротивление. Вскоре Михайлова перевели в СИЗО «Лефортово», где он находится и сейчас.

К моменту ареста сорокалетний Сергей Михайлов руководил 2-м управлением ЦИБ, то есть фактически курировал и хакеров, сотрудничающих с ФСБ, и расследования взломов, связанных с государственной безопасностью. Он часто выезжал на конференции по кибербезопасности, где рассказывал о том, как в России ловят кардеров.

Михайлову предъявили обвинение в госизмене. Вскоре выяснилось, что связано оно может быть с тем, что именно сотрудник ФСБ раскрыл американским спецслужбам имена российских разведчиков, курировавших атаку на США. Уже после его ареста *The New York Times* писала [\[243\]](#), что ключевую помощь в поиске хакеров американским спецслужбам оказали источники в России. У Михайлова был доступ к подобным данным; мой источник рассказывал, что у главы 2-го управления ЦИБ ФСБ было много претензий к методам ГРУ: он считал, что там «ломают серверы нагло, топорно и грубо», а следы атак «всегда видны».

Через некоторое время выяснилось, что Михайлов, видимо, был не первым, кого сотрудники ФСБ задержали по этому делу. За день до его ареста, 4 декабря 2016 года, один из топ-менеджеров «Лаборатории Касперского» Руслан Стоянов приехал в московский аэропорт, чтобы вылететь в командировку в Китай. Зарегистрировавшись на рейс, Стоянов отправил об этом SMS жене. На мероприятии в Китае, где его ждали, он на следующий день, однако, не появился. Организаторы поездки [сообщили](#) руководству «Лаборатории Касперского», что Стоянов пропал. Через несколько дней компания сообщила, что нашла сотрудника в СИЗО «Лефортово», куда его доставили сотрудники ФСБ.

Стоянов многие годы занимался кибербезопасностью: в начале 2000-х дослужился до звания майора в управлении «К» при Министерстве внутренних дел, работал в отделе безопасности «РТ-Комм.ру» (дочерняя структура «Ростелекома», в 2016 году [предоставляла](#) услуги связи ЦИБ ФСБ). Потом создал компанию, которая сначала занималась самостоятельными расследованиями, а в 2012-м [вошла](#) в состав «Лаборатории Касперского», где Стоянов возглавил отдел расследования компьютерных инцидентов. «Это был созданный внутри департамент, который обслуживал ФСБ и МВД, —



рассказывал бывший высокопоставленный сотрудник компании. — Сами они себя называли „орки“, им очень нравилось это название».

По словам Евгения Касперского, Стоянов «очень плотно работал с Центром информационной безопасности ФСБ». «Орки» сопровождали группы захвата, когда те задерживали киберпреступников. «Прямо вместе с эфэсбешниками выезжали на точку и не стеснялись этого, Стоянов выкладывал фотоотчет о том, как они захватывали группировку *Lurk* (см. главу 15. — Прим. Авт.)», — вспоминал один из сотрудников «Лаборатории Касперского».

Задержали Стоянова по делу о госизмене. Видимо, его подозревают в том, что именно он передавал американцам информацию, полученную от Михайлова и Дмитрия Докучаева — еще одного сотрудника ЦИБ ФСБ, которому также предъявлены аналогичные обвинения.

Докучаев, похоже, один из первых российских хакеров, который перешел на постоянную работу в спецслужбы. Компьютерами он увлекался с юности и одновременно, как и многие подростки, сочинял стихи. В 2001 году он, например, написал такие строки:

*Linux — Rules, Винда — маздай форева. Так говорили мне друзья. Проверить я решил, купив редхат нулевой. Живя во грезах, диски формата. Вдруг непонятные экраны и таблицы: Тут нужен своп, а здесь — резервный диск. Смотрю я книги, листаю все страницы... Как кто-то говорил: «без бутыля не обойтись». Уф... Разобрался... Идет формат разделов. Мне нужно выбрать компоненты для инсталла. Я уж не соображаю, башка вся запотела. Весь выложился тут, а Linux'у все мало. Проходит час-другой, Ура! удача! Setup complete. со второй попытки. Волнуясь, радуясь, я от счастья плачу. Нет! Это не RedHat, а просто пытка...*

Докучаев родился в Каменске-Уральском — городе в часе езды от Екатеринбурга. Последний раз Каменск-Уральский попадал в новости в 2013 году — после того, как там появилась [\[244\]](#) радикальная группировка, преследовавшая гомосексуалов (однажды они приехали с мужчиной на кладбище, заставили его вырвать из земли надгробие, а потом преследовали его на джипе — такие операции активисты называли «сафари»). Сам хакер описывал родной город так: «Насчитывает 200 тысяч жителей, что совсем немного. В Каменске-Уральском очень много заводов, как правило, по металлообработке, — трубный, металлургический, алюминиевый. Городу скоро стукнет 300 лет. Не такой и старый, но уже и немолодой. Немного о достопримечательностях: это, конечно, вам не Москва, но в Каменске есть краеведческий музей, очень много театров, библиотек, стадионов, спорткомплексов и интернет-кафе».

В последних Докучаев в юности и проводил большую часть своего времени — много играл в видеоигры: *Worms Armageddon*, *Need for Speed*, *Quake 3*. Свой первый взлом он совершил в городской сети, чтобы получить бесплатный доступ в интернет. «Я всегда считал, что информация должна быть свободной, поэтому платить провайдеру



за предоставление доступа ужасно не хотелось», — вспоминал [\[245\]](#) он.

После школы Докучаев поступил в политехнический институт в Екатеринбурге на факультет информационных систем в технике и технологиях; позже стал работать системным администратором на кафедре одного из екатеринбургских университетов. О себе он подробно рассказывал на своем сайте [\[246\]](#) (сейчас удален), который назывался «*Dmitry's homepage. The best...*». В 2002 году он без стеснения писал, что «приобретает популярность в инете и не только;» Сотрудничаю с редакцией журнала „Хакер“ и получаю приличный гонорар;»). Свой ник — *Forb* — он образовал от английского слова *forbidden*, «запрещенный».

В журнале, например, вышел его материал «10 роковых ошибок хакера»: «Хакер — как сапер, первый раз ошибается при выборе своей профессии. Каждый взлом может оказаться для него фатальным, и сам он это осознает. Но не может с этим смириться, считая взлом экстремальным видом спорта. Если ты все еще раздумываешь, «быть или не быть хакером», то я дам тебе совет. НЕТ! Быть хакером уже не так модно, да к тому же опасно. Так что займись лучше чем-нибудь другим, например, продажей школьных выпускных сочинений по русскому языку через интернет:»).

Кроме раздела с найденными программными уязвимостями, на сайте Докучаева был и раздел с его фотографиями: «Я на диване (1997 год)» [\[247\]](#) (подросток в клетчатой фланелевой рубашке и спортивных штанах сидит на диване), в МИФИ, в Крыму, на дискотеке у Черного моря.

В 2004 году Докучаев занимался кардингом и взламывал сайты по заказу — о том, как это делать, он подробно рассказывал на собственном сайте. Своим главным достижением хакер считал взлом одного из правительственных сайтов США. В 2006-м переехал в Москву и стал [\[248\]](#) работать в «Хакере» как штатный сотрудник.

Знакомые Докучаева вспоминали, что после переезда он женился на девушке, которую вскоре научил взламывать сайт русского *Cosmopolitan*. Хакер и его коллеги много веселились и выпивали вместе, иногда попадая в истории. «Беспредел доходил даже до криминала, клево было, все пати и встречи проходили спокойно, но весело», — вспоминал один из них. Как-то во время очередной пьянки Докучаев посадил его на трехметровую высоту, чтобы сломать камеру видеонаблюдения. После этого они убегали от полицейских — и наткнулись на сотрудника ФСБ, от которого хакер «получил в челюсть».

Вскоре Докучаев и сам стал сотрудничать с ФСБ, а потом и перешел туда на работу, став старшим оперуполномоченным 2-го отдела оперативного управления ЦИБ ФСБ — департамента, занимающегося киберзащитой государства и расследованием хакерских дел, связанных с угрозой безопасности страны. Там он трудился до 2016 года, пока его не арестовали.



Один из хакеров, периодически работающих на спецслужбы, сказал мне, что в ФСБ считают: США атаковали хакеры, нанятые ГРУ, но не штатные сотрудники разведки. При этом он уверен, что за Михайловым и Докучаевым следили еще с весны 2016 года.

В апреле 2018 года Докучаев подписал досудебное соглашение о частичном признании вины в передаче данных иностранным спецслужбам. В соглашении, видимо, говорится о передаче данных не о государственных хакерах, а о кардерах. Достоверно узнать, действительно ли сотрудники ФСБ, ранее курировавшие хакеров, сдали их американским спецслужбам, почти невозможно. Судебные процессы по статьям, связанным с госизменой, всегда закрыты от журналистов. В конце февраля 2019 года Михайлова и Стоянова признали виновными в госизмене и приговорили к 22 и 14 годам заключения. В чем именно состояло обвинение, видимо, навсегда останется тайной. Иначе выйдет, что Россия признается в организации кибератак на США.



## Глава 32

### Чистосердечное признание

Единственный человек, который публично заявил, что совершал атаки на США, — хакер Константин Козловский. Он земляк Дмитрия Докучаева — родился в том же Каменск-Уральске — и бывшая «цель» Руслана Стоянова: Козловский был одним из тех, кого арестовали по делу группировки *Lurk*, похищавшей деньги из российских банков (см. главу 15).

С 14 августа 2017 года Козловский, который к тому времени уже год находился под арестом за создание самой успешной хакерской группировки 2010-х, начал выкладывать в фейсбуке посты о работе на ФСБ. Как он получил доступ к социальным сетям, находясь в СИЗО «Лефортово», подконтрольном спецслужбе, неизвестно. Публикуя посты, он часто использовал хэштеги вроде #разоблачения, #cyberwar, #russianhacker #Взлом\_Демпартии\_США и заявлял, что хочет «справедливости». «Мне не верят, так как очень выгодно засудить нас за те суммы, которые осели в каких-то других карманах, — объяснял он. — Мои показания никому неинтересны, так как, видимо, нарушают планы больших людей». Верифицировать его версию событий невозможно: публикации легко могут быть частью операции спецслужб.

Суд по делу Козловского проходил в закрытом режиме — журналистов туда не пускали, но неизвестные записали заседания на диктофон, а потом выложили [\[249\]](#) в открытый доступ. На первом заседании хакер заявил, что многие годы работал на государство.

— Ваша честь! Мой куратор из ФСБ — Дмитрий Докучаев, — сообщил он. — Если это возможно, прошу пригласить его в зал судебного заседания. Хочется посмотреть ему в глаза, так как из-за него много людей находится под стражей. Докучаев в настоящее время арестован и находится в СИЗО «Лефортово».

Суд отказался вызывать Докучаева. В следующем выступлении Козловский рассказал, что выполнял различные задания сотрудников ФСБ, в том числе взламывал электронную почту сотрудников Национального комитета Демократической партии США, переписку Хиллари Клинтон и американские военные предприятия.

«Все западные СМИ говорят про [взломы]. Однако я хочу сказать, если я в чем и виноват, то только в том, что работал на это государство, — заявил он. — Другие [арестованные участники *Lurk*] ни в чем не виновны, они еще вчера на кнопки нажимали, а теперь сидят в тюрьме. У меня болит сердце за то, что я их подставил, а также за то, что сотрудники ФСБ с нами так поступают».

По словам Козловского, сотрудничать с Докучаевым и ФСБ он начал в 2008 году, когда ему было 16 лет, и выполнял все указания своих кураторов. Подробно об истории своих отношений со спецслужбами он рассказал в письме, которое выложил в своем фейсбуке:



Занимаясь компьютерными технологиями, я общался на многочисленных интернет-форумах. В 2008 году я вступил в диалог об уязвимостях почтовых сервисов. В процессе обсуждения у меня завязался спор на 500 \$ США, в результате которого я продемонстрировал уязвимость на примере одного email, выложив пароль на общее обозрение в форум. Далее я потребовал деньги у спорщика, предложив встретиться. В установленном месте ко мне подошли 2 человека. Определив, что я и есть человек, взломавший почту, мне предъявили удостоверение сотрудника ФСБ и настойчиво попросили сесть в автомобиль.

Меня привезли, как я потом узнал, во внутренний двор управления ФСБ по Свердловской области (г. Екатеринбург). В помещении 3 на 3 метра я провел двое суток. Еды не дали. Только 2 раза воды в алюминиевой миске. Для справления нужды принесли ведро. Сотрудники ФСБ дали выбор: работать с ними или отправить в тюрьмы за взлом почты. Я согласился, подписав бумагу.

За годы сотрудничества я выполнил множество заданий. Илья – мой куратор (позже на суде он укажет, что имел в виду сотрудника ФСБ Дмитрия Докучаева. — Прим. Авт.) : давал задания и контролировал меня, снабжал техническими и программными средствами, покровительствовал в вопросах с правоохранителями.

В последние годы фокус внимания был прикован к серверам Америки и ЕС. Поручения по взлому Национального комитета Демократической партии США, переписки Хиллари Клинтон, я выполнил успешно, передав данные на жестком диске сотруднику ФСБ Илье (850 ГБ в сжатом виде с видеозаписями взлома).

Козловский называл атаки «мероприятиями», пользуясь терминологией спецслужб. «В отношении США и стран ЕС мероприятия затрагивали получение доступов (взлом) к крупнейшим промышленным предприятиям, государственным и военным структурам, финансовым учреждениям (банки / биржи), спортивным организациям (FIFA, Олимпийский комитет, WADA), АЭС, ГЭС, ГРЭС, крупнейшим СМИ и их аккаунтам в соцсетях», — писал он. Козловский рассказывал, что «однажды по поручению ФСБ я сделал вброс о смерти Горбачева М.С. в микроблоге РИА Новости»; такой случай действительно был [\[250\]](#) 8 августа 2013 года. Он также утверждал, что по распоряжению ФСБ находил персональные данные исследователей катастрофы «боинга», который в 2014 году был сбит неподалеку от Донецка, и взламывал их компьютеры.

В какой-то момент, по словам Козловского, спецслужбы требовали от него создать «красную кнопку»: техническое решение, позволяющее им провести массированное разрушение критической инфраструктуры — заводов, АЭС, бирж — в США и Европе. Козловский отказался, решив, что не хочет «иметь отношение к началу тре-



твей мировой войны». Через некоторое время его снова попросили о том же — он снова отказался, а в ответ услышал: «Хорошим твой отказ не закончится». После этого сотрудник ФСБ, курировавший его, пропал. Вскоре Козловского задержали и военным самолетом Росгвардии доставили в Москву. По его словам, компьютеры и другие вещественные доказательства, подтверждающие его рассказ, находятся в распоряжении ведомства.

В апреле 2017 года Козловский написал письмо директору ФСБ Александру Бортникову, в котором рассказал, что «верил, что действует в интересах государства» и был вынужден предать огласке свое участие в атаках на зарубежные страны только потому, что следователи обещают ему пожизненное заключение.

Хакеры, сотрудничавшие со спецслужбами, говорят, что большие операции вроде тех, о которых рассказывает Козловский, не могут проводить одиночки и что его история выглядит реалистично только в части, посвященной вербовке. «Обычно по таким инфраструктурам трудятся целые киберармии и отделы, которым нужно найти уязвимости нулевого дня в защите — тем более в таких хорошо защищенных объектах, как военные или критические объекты», — объясняет один из завербованных хакеров. Другой хакер указал, что международными кибероперациями занимается ГРУ, а сфера ответственности ФСБ — только внутрироссийские дела.

Докучаев заявил, что не знаком с Козловским, и отверг обвинения; не фигурировала фамилия Козловского и ни в одном из официальных американских расследований.

В конечном счете до сих пор никто так и не предъявил окончательных доказательств того, что американских политиков взломали именно российские хакеры, как и того, что эти люди были связаны с Кремлем. «Нет никаких нормальных технических отчетов. В некоторых говорится о том, что взломы происходили по часовому поясу, который соответствует Москве. Ну и мотивация могла быть. Но мотивация — это не доказательство, — объясняла на одной из конференций по кибербезопасности криминалист Веста Матвеева из компании *Group-IB*, занимающейся в России расследованиями киберпреступлений — часто совместно со спецслужбами. — Еще говорят, что сервер находился в России. Но какой нормальный хакер будет атаковать со своего компа выборы в США? Русские строки в коде — тоже не очень доказательство. Как мы знаем, северокорейская группировка *Lazarus*, чтобы запутать след, использовала в коде русские слова — *nachalo*, *vykhodit*, *poluchit*, *derzhat* и так далее. Можно ли доказать, что это все-таки русские? Можно. Всегда можно дойти до конкретных людей, но сейчас политика этому мешает. Если весь мир начнет расследовать, все страны будут предоставлять данные с серверов и VPN, то — получится».



## Глава 33

### Моя цифровая оборона

Как и в каждой войне, в киберконфликтах важна не только атака, но и оборона. До последнего времени российское государство практически не вело речи о необходимости оборонять государственные сайты и критическую инфраструктуру — атомные электростанции, военные заводы, системы снабжения и прочие объекты, успешные атаки на которые могут вызвать экологическую или финансовую катастрофу и привести к человеческим жертвам. В последние годы отношение изменилось, вероятнее всего, из-за постоянных новостей о хакерских проникновениях на жизненно важные объекты (например [\[251\]](#), на американскую АЭС), развития кибершпионажа и роста киберугроз со стороны террористических организаций.

«Думаю, документ о неприменении кибероружия скоро подпишут, — сказал мне один из сотрудников компании, связанной с защитой государственной критической инфраструктуры. — Но только после того, как произойдет какая-нибудь по-настоящему большая катастрофа». Правда, вирус *NotPetya* поразил компьютеры по всему миру уже после этого разговора — а никакой международной инициативы в области кибероружия так и не появилось.

Мой собеседник, занимающийся информационной безопасностью критической инфраструктуры, говорит, что на стратегически важных российских объектах часто находят «лишнее». «Обсуждаем с людьми оттуда, что у них проблема, но они не признают, что у них что-то может пойти не так. Говорят: ну это просто вирус с целью кражи денег, — рассказывает он. — Но ведь он оказался в закрытой инфраструктуре! И им повезло, что вирус с таким функционалом. А если бы у него была другая задача?»

Правоохранители и аффилированные с ними компании время от времени рассказывают о кибератаках на российское государство — видимо, сильно реже, чем они реально происходят. Например, в 2013 году против России было применено кибероружие *Sputnik* (узнать об этом можно из исследования [\[252\]](#) научно-производственного объединения «Эшелон», которое занимается сертификацией иностранного программного оборудования для Министерства обороны). Программа занималась кибершпионажем — собирала информацию о деятельности военных ведомств, институтов, дипломатических организаций, используя уязвимости «нулевого дня» в приложениях *Word*, *Excel* и *Outlook* для *Windows*. Отследить, куда стекались украденные сведения, не удалось: пункт назначения скрывала цепочка прокси-серверов. Сотрудники «Эшелона» поясняли, что украденные сведения могли быть интересны геополитическим врагам России, и заключали: «Кибервойны как форма проявления межгосударственного противостояния вошли в активную фазу».

В июле 2016 года ФСБ сообщила [\[253\]](#) об обнаружении троянов в информационной инфраструктуре правительственных, научных и оборонных учреждений страны (всего около двух десятков предпри-



ятий). Ведомство указывало, что атака была тщательно спланирована и осуществлялась на высоком профессиональном уровне. Под каждое предприятие писался [254] свой эксплойт, жертв заражали с помощью фишинга. После заражения программа подгружала необходимые модули, которые позволяли дистанционно включать веб-камеры и микрофоны, перехватывать сетевой трафик, сохранять данные о том, что пользователи набирали на клавиатуре. В парламентском комитете по безопасности тогда заявили [255], что подобный кибершпионаж «выгоден прежде всего американцам».

С помощью фишинга китайские прогосударственные хакеры годами атакуют [256] российские военные ведомства. «Данная группа работает еще с 2008 года. — указывали в отчете специалисты *Positive Technologies*. — С почтового ящика действующего офицера Минобороны России, к которому получили доступ хакеры, отправлялась рассылка с вредоносным вложением». В письмах говорилось о «компенсации военнослужащим за аренду жилья» и «повышении зарплаты военнослужащим». После заражения хакеры могли следить за зараженными компьютерами, скачивать с них информацию, делать скриншоты экрана, активировать микрофон и веб-камеру. Такие взломы могут не только привести к утечке секретных документов, но и дать хакерам доступ к критической инфраструктуре, что, в свою очередь, может быть использовано и для серьезных провокаций, и для начала кибервойны.

Сейчас, чтобы защитить свое общение в интернете, российские чиновники используют [257] закрытую государственную сеть *RSNet*. У каждого сотрудника есть защищенная рабочая почта, на которую можно зайти только с определенного IP и с определенного компьютера, но далеко не все соблюдают необходимые предписания, особенно если речь идет о высших эшелонах власти. Постепенно государство начинает задумываться и о защите телефонных разговоров: один из НИИ, работающих на российские спецслужбы, в 2017 году выпустил [258] «криптотелефон», позволяющий шифровать звонки.

\*\*\*

Российский аналог американского Агентства национальной безопасности, ФАПСИ, появился [259] в начале 1990-х. Ведомство было создано на основе 8-го управления КГБ СССР, отвечавшего в том числе за правительственную связь и засекречивание информации в интересах высших органов власти (именно там работал и играл с друзьями в шахматы Михаил Масленников; см. главу 28). Один из руководителей ФАПСИ Владимир Маркоменко во время выступления в Госдуме в 1996 году говорил [260], что «спецслужбы США постоянно предпринимают усилия по добыче сведений об информационно-телекоммуникационных комплексах других стран, в том числе и России», и прямо указывал, что в российских госорганах спустя рукава относятся к информационной безопасности.



Маркоменко считал, в мире давно идет «информационная война» и Россия не может оставаться от нее в стороне. «Боевые действия» в этой войне чиновник представлял себе так: «подавление инфраструктуры систем обороны противника, его информационных и телекоммуникационных систем», «перехват информации», «взлом информационных ресурсов противника», «борьба за общественное мнение путем распространения по информационным каналам противника и глобальным сетям дезинформации или тенденциозной информации для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения». Фактически все его предсказания сбылись.

Оценить эффективность работы ФАПСИ трудно. Сотрудник ведомства рассказывал [\[261\]](#), что, работая администратором в компьютерном клубе, зарабатывал в два раза больше — но пошел служить государству, чтобы получить «ксиву» и «некоторую свободу действий»: «Можно помаленьку ломать, на небольшие проделки глаза, естественно, закрываются». ФАПСИ расформировали в 2003 году; часть подразделений перешли в состав ФСБ, другие — в ФСО.

\*\*\*

Специалисты по информационной безопасности годами предупреждали, что хакеры смогут найти способ нанести настоящий физический урон критически важным объектам. В 2009 году это случилось, когда против Ирана применили *Stuxnet*, кибероружие, разработанное специально для того, чтобы помешать ядерной программе исламской республики. Как писал [\[262\]](#) журналист *The New York Times* Дэвид Сэнгер, целью создания *Stuxnet* было мирное решение возможной проблемы: США опасались, что Израиль начнет бомбардировки Ирана и его ядерных объектов.

Источники указывали [\[263\]](#), что *Stuxnet* создали спецслужбы сразу нескольких государств: ЦРУ, АНБ и кибернетическое командование США, Центр правительственной связи Великобритании, спецподразделение радиоэлектронной разведки израильского МОССА-Да. Чтобы осуществить свои планы, спецслужбы сначала атаковали [\[264\]](#) пять иранских компаний, связанных с заводом по обогащению урана. После этого *Stuxnet* попал на флеш-накопители сотрудников и они, сами того не зная, заразили защищенную сеть завода, не подключенную к интернету. Когда *Stuxnet*, спроектированный специально под систему управления предприятиями, связанными с ядерной энергетикой, попал в систему завода по обогащению урана в Натанзе, он уничтожил более четверти всех его центрифуг, докачав к программному обеспечению дополнительный вредоносный код, который изменил поведение устройств.

Центрифуги приводились в движение электромотором и вращались со скоростью 1000 оборотов в секунду. *Stuxnet* увеличивал эту скорость до 1400 оборотов, а потом резко сбрасывал — в результате центрифуги разрушались. При этом инженеры завода, находящиеся



в соседнем помещении, видели на своих экранах, что все процессы в норме. Они долгое время не понимали, в чем причина аварий; некоторых из них уволили, подозревая в нарушении правил эксплуатации.

После атаки *Stuxnet* продолжил распространяться в других странах: в 2010 году он заразил около 100 тысяч компьютеров по всему миру, в том числе проник в систему одной из российских атомных станций. Как и иранские заводы, АЭС не подключены к интернету, и заражение одной из станций могло свидетельствовать о серьезных проблемах с их безопасностью.

С тех пор появились новые виды кибероружия, действующие похожими способами. Так, в 2016 году эксперты компании *ESET* сообщили о появлении программы *Industroyer*, цель которой — вмешиваться в критические процессы в системах управления энергокомпаний: с ее помощью хакеры могли управлять выключателями на подстанциях. «Способность *Industroyer* влиять на работу промышленного оборудования делает ее наиболее опасной угрозой со времен *Stuxnet*», — заявляли в компании. Эксперты предполагают, что *Industroyer* могла быть причиной сбоя электроснабжения в Киеве в декабре 2016 года. Тогда свет пропал в четырех районах города.

23 июня 2017 года газета *The Washington Post* рассказала [\[265\]](#), что Барак Обама, когда еще был президентом США, поручил Агентству национальной безопасности разработать кибероружие против России в качестве ответа на предположительное вмешательство в американские выборы. Спецоперация предполагала внедрение в российскую электронную инфраструктуру «имплантов», которые в нужный момент смогут вывести ее из строя; журналисты называли их «цифровым аналогом бомб». Америка не первый год использует эту технологию: бывший директор АНБ и ЦРУ Майкл Хайден говорил [\[266\]](#), что США установили в 2010-х «импланты» на десятки тысяч компьютеров по всему миру, «которые можно использовать, когда будет необходимо».

\*\*\*

Еще в конце 1990-х чеченские террористы атаковали [\[267\]](#) российские государственные ресурсы и СМИ. 13 декабря 1999 года они взломали главную страницу новостного агентства ИТАР-ТАСС; через пару месяцев — разместили на главной странице РБК текст с угрозами в адрес россиян и исполняющего обязанности президента Владимира Путина.

Почти двадцать лет спустя кибератаки продолжают оставаться одним из направлений деятельности радикальных группировок, но теперь речь идет о более серьезных угрозах, чем просто взлом сайта в интернете. «Россия из-за участия в военных операциях на Ближнем Востоке сильно раздражает террористов, — заявил на конференции по безопасности 30 июня 2017 года Илья Сачков из компании *Group-IB*, занимающейся информационной безопасностью. —



Мы, к сожалению, уже в этом году столкнемся с успешной атакой на критически важную инфраструктуру» (примерно во время его рассказа происходила крупнейшая хакерская атака в истории, распространение вируса *NotPetya*, — подробнее о ней в главе 35).

Через год после того, как лидер «Исламского государства» провозгласил создание «халифата» на территории Сирии и Ирака, внешняя пропаганда группировки сильно изменилась: вместо постов и видео, в которых новобранцев агитировали воевать на стороне ИГ, начали появляться материалы с призывами помочь в строительстве нового государства, которому требовались врачи, учителя, журналисты, программисты. Примерно в это же время в ИГ появилось хакерское подразделение — *ISIS Hacking Division*<sup>264</sup> [268] или «Киберхалифат». Его организовал переехавший из британского Бирмингема хакер Трик (*TriCk*).

У Трика к тому времени был большой опыт: свой первый взлом он совершил [269] в 11 лет, чтобы отомстить сопернику по онлайн-игре, а в 15 собрал хакерскую группировку *Team Poison*. Целью ее было не зарабатывание денег, но сопротивление: Трик считал необходимым бороться за права палестинцев и жителей Кашмира — и в рамках этой борьбы вместе с товарищами атаковал израильские и американские медиа и соцсети, например, размещая собственные лозунги и предупреждения на главных страницах идеологически враждебных сайтов.

*Team Poison* нападала на сайты НАТО, Министерства обороны Великобритании, аккаунт Марка Цукерберга в фейсбуке. В 2012 году после взлома [270] почты помощника бывшего премьер-министра Великобритании Тони Блэра Трика нашли и арестовали — хакером оказался Джунейд Хуссейн, сын пакистанских эмигрантов. Проведя полгода в английской тюрьме, он уехал в столицу ИГ Ракку, где взял себе имя Абу Хуссейн аль-Британи и стал главным хакером группировки.

В этом качестве он продолжал делать то, что умел лучше всего, — взламывал американские сайты и соцсети. Например [271], в январе 2015 года Хуссейн разместил в твиттере американского центрального военного командования пост «Солдаты США, мы идем, берегитесь». Хакер раскрывал личности и адреса американских военных в США, призывая сторонников найти их и убить. Летом 2015 года Трик раскрыл личности двух активистов, борющихся с пропагандой ИГ в интернете; их казнили. В начале августа 2015-го 21-летний Хуссейн оказался на третьем месте в списке [272] Пентагона на уничтожение — после лидера «халифата» Абу-Бакра Аль-Багдади и палача ИГ, называвшего себя Джихадистом Джоном.

Через несколько дней после этого агент под прикрытием связался с хакером в защищенном мессенджере *Surespot* (Трик публиковал свои контакты в твиттере, чтобы с ним могли переписываться единомышленники). Во время разговора он скинул Хуссейну ссылку на страницу, с которой в телефон хакера загрузился вирус. После этого его смогли отследить — и дрон сбросил на Хуссейна бомбу.



Агентом под прикрытием оказался хакер *Shm00p*, после смерти Трика он написал [273]: «Я, блядь, виновен, мне жаль, я играл в игру, в которую не должен был [играть]». Он утверждал [274], что помог спецслужбам из-за того, что те угрожали его семье, и говорил, что его обманули. «Я помог вам его УБИТЬ. Как вы думаете, удастся мне теперь поспать ночью? — писал *Shm00p*. — Он был террористом и животным, но я чувствую, что меня предали».

Несмотря на смерть Хуссейна, специалисты по информбезопасности вскоре стали замечать на подпольных форумах по всему миру рост интереса террористических группировок к хакерским атакам, в особенности на критическую инфраструктуру. Об этом рассказывает собеседник, исследующий площадки общения хакеров; эту информацию подтверждает [275] один из отчетов *Group-IB*. Сотрудник российских спецслужб рассказывал мне, что пользователи, выходящие с сирийских IP, предлагают специалистам по кибербезопасности работу и интересуются методами ведения кибервойны. Сообщения на форумах они пишут в основном через *Google Translate*. Кроме того, террористов интересуют способы проникнуть в системы оборонных предприятий, чтобы украсть секретные разработки. Как рассказывал *The New York Times Magazine*, уже многие годы различные группировки ищут [276] красную ртуть — выдуманную военную разработку СССР, которую якобы можно использовать для создания оружия массового поражения.

«Если игиловцы на самом деле поймут, где покупать уязвимости нулевого дня, то начнут происходить не самые хорошие события», — говорит специалист по безопасности критической инфраструктуры. «Человечество борется с терроризмом с XIX века, — объясняет специалист по информационной безопасности Илья Сачков. — Наука о защите киберпространства появилась более-менее около 20 лет назад, но серьезно с терроризмом в интернете мы никогда не встречались. Только с точечными атаками — как на Украине».

\*\*\*

Успех *Stuxnet* в борьбе с иранской ядерной программой не остался незамеченным в России. В январе 2013 года Владимир Путин поручил [277] ФСБ создать государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Идея заключалась в том, чтобы «накрыть» все государственные информационные ресурсы колпаком единой системы с постоянным мониторингом всего периметра — отслеживать всю входящую информацию из интернета. К этой системе решили подключить все ресурсы и объекты критической инфраструктуры, чтобы они обменивались информацией об атаках с главным центром — он должен был определять, как устроена атака, и направлять рекомендации о безопасности другим участникам ГосСОПКА.

Концепцию системы утверждали два года. В 2015 году ФСБ опубликовала [278] выписку из нее. Там указывалось, что ГосСОПКА



будет разделена на центры реагирования в разных регионах и ведомствах и что при ФСБ создается Национальный координационный центр по компьютерным инцидентам (Gov-CERT), который займется обороной критической инфраструктуры. Возглавил Gov-CERT сотрудник ФСБ Алексей Новиков; по его словам, к ноябрю 2016-го к системе были подключены десять госорганов, ведомственные центры реагирования уже запустили Центробанк и «Ростех» [\[279\]](#).

Новиков объяснял [\[280\]](#), что сейчас спецслужбы выстраивают обмен информацией об инцидентах между госорганами. По его словам, в системе будет предусмотрен специальный режим, в котором сообщение об инциденте можно будет отправить в центр вместе с «запросом на оказание содействия». Такие сообщения будут иметь высший приоритет, дежурная смена Национального координационного центра по компьютерным инцидентам их сразу увидит и начнет действовать: например, привлечет провайдеров к фильтрации вредоносного трафика или попытается прекратить функционирование бот-сетей. Чиновник утверждает, что еще в 2014 году во время Олимпиады в Сочи ФСБ удалось вывести из строя несколько центров управления бот-сетями.

Кроме того, ФСБ требует, чтобы госслужащие внимательнее относились к электронным письмам. «Одна из госкорпораций получила несколько [подозрительных] писем, сотрудники службы безопасности переслали их нам на исследование, — рассказывал Новиков на Уральском форуме по информационной безопасности в феврале 2017 года. — Мы провели экспресс-анализ и обнаружили известное семейство [вирусов]. Мы смогли установить, откуда были отправлены письма. Оказалось, что они ушли еще на 10 объектов, но мы смогли предотвратить атаку».

В декабре 2016 года премьер Дмитрий Медведев внес в Госдуму законопроект о безопасности критической информационной инфраструктуры, который обязывает все объекты обмениваться данными с ГосСОПКА. Документ не только предполагает создание специального реестра для компьютерных систем, использующихся на критически важных объектах, но и предусматривает новую уголовную статью за атаки на критическую информационную инфраструктуру. Максимальное наказание по ней — 10 лет тюрьмы, причем получить его могут не только хакеры, но и те госслужащие, из-за попустительства которых произошла утечка или атака.

По мнению ФСБ, курировавшей законопроект, если быстро не предпринять шаги по защите инфраструктуры, террористы и иностранные спецслужбы будут угрожать стабильности страны: Россия «поставлена в прямую зависимость от безопасности функционирования информационно-телекоммуникационных сетей и информационных систем». «При развитии событий по наихудшему сценарию компьютерная атака способна полностью парализовать критическую информационную инфраструктуру государства и вызвать социальную, финансовую и (или) экологическую катастрофу», — говорилось [\[281\]](#) в пояснительной записке ФСБ к законопроекту. В каче-



стве примеров возможных сценариев атак в документе упоминались *Stuxnet* и «паралич работы нескольких крупных финансовых учреждений Южной Кореи в марте 2013 года».

От ФСБ законопроект и критическую безопасность инфраструктуры курирует заместитель директора ведомства Дмитрий Шальков. В январе 2017-го он заявил, что за прошлый год из-за рубежа российские информационные ресурсы атаковали 70 миллионов раз (Владимир Путин называл [282] эту же цифру, говоря о 2015 годе). «Российская инфраструктура постоянно подвергается хакерским атакам. В ноябре 2016 года совершалась массированная атака на финансовый сектор страны. Объектами стали Сбербанк, „Альфа-банк“, „Банк Москвы“ и другие. Атаки были нейтрализованы специалистами по информационной безопасности ФСБ. Количество атак на официальные ресурсы России неуклонно растет», — объяснял [283] Шальков, представляя законопроект в Госдуме.

В первом чтении его приняли [284] 27 января 2017 года — однако второе чтение многократно откладывалось. 23 июня глава ФСБ Александр Бортников попросил [285] депутатов ускорить принятие законопроектов о критической инфраструктуре; через две недели, 7 июля 2017, документ прошел второе чтение, а вместе с ним приняли [286] поправку к закону о гостайне — к таким сведениям добавились меры обеспечения безопасности критической информационной инфраструктуры и ее защищенности от кибератак. Через несколько дней закон подписал Владимир Путин.

В феврале 2019 года российские власти решили изолировать российский сегмент интернета и фильтровать весь входящий интернет-трафик. Теперь при необходимости власти смогут отключить весь «внешний интернет», то есть все сайты, находящиеся не на российских серверах. Технический директор «Роскомсвободы», организации, которая следит за соблюдением свободы слова в сети, считает [287], что этот шаг — еще одна часть стратегии, с помощью которой власть пытается обезопасить себя от протестов: их участники обычно координируют действия именно через интернет.

\*\*\*

Средства для защиты критической инфраструктуры выпускают многие коммерческие компании: *Positive Technologies*, «Лаборатория Касперского», *Group-IB* [288]. Одна из них, «Информзащита», много лет работает с государством: например, она занималась обеспечением безопасности транспорта во время Олимпиады в Сочи. Журнал *Forbes* сообщал [289], что «Информзащита» за пять лет заключила четыре с половиной сотни контрактов с госзаказчиками на общую сумму в пять миллиардов рублей.

Основатели «Информзащиты» — выходцы из Генерального штаба и военных НИИ (в том числе из «Кванта»). В конце 1990-х они начали устанавливать свои системы защиты в российской Центральной избирательной комиссии и Центробанке; в 2000-х — выпу-



стили средство защиты сетей и шифровки данных «Континент», которое используется [290] многими государственными органами. Тогда же в «Информзащите» появился отдел «пентестеров» — перед тем как продать свои программы заказчику, компания тестировала устойчивость его систем.

С «Информзащитой» среди прочих работала [291] Алиса Шевченко — на ее компанию «ЦОР Security» Минфин США в декабре 2016 года наложил санкции за вмешательство в президентские выборы.

В своем инстаграме Шевченко называла [292] себя «еще одной миленькой девочкой-хакером». Знакомый Шевченко описал ее как одну из самых способных «пентестеров» России, которая может взломать почти любую систему. По его словам, Шевченко очень много работает, а все свободное время проводит за чтением специальной литературы. На ее сайте указано, что девушка «чаще всего работает над уязвимостями и эксплойтами». Весной 2014 года на ежегодном форуме российских хакеров *Positive Hack Days* она с легкостью взломала систему управления инфраструктурой города-полигона; его защиту она назвала «тривиальной».

Шевченко начинала [293] свою карьеру, работая вирусным аналитиком в «Лаборатории Касперского»; после этого она организовала собственную компанию *Esage*, которая специализировалась на анализе киберзащиты различных организаций. Заказы компания получала от интегратора «ДиалогНаука», который обслуживал контракты Федеральной службы охраны и Минобороны. Позже *Esage*, переименованная в «Цифровое оружие и защита», начала заниматься тестами на проникновение, используя для этого фишинговые письма и вредоносные сайты (то есть те же методы, что и те, кто взламывал американских политиков и международных спортивных чиновников).

Работали с Шевченко около десяти человек — их всех девушка нашла на хакерских форумах. Вместе, как указывал [294] *Forbes*, они занимались разработкой инструментария для взломов. Власти США считают [295], что компания Шевченко предоставляла свои исследования и разработки ГРУ. «Проснулась от тонны запросов о каком-то списке, о котором никогда не слышала, — написала Шевченко на следующий день после объявления Минфина США в твиттере. — Кажется, не выйдет сегодня покодить...» Знакомый Шевченко сказал мне, что она уехала из России; сайт [296] ее компании перестал открываться.



## Глава 34

### Всемирный вымогатель

Офис «Лаборатории Касперского» находится на берегу Химкинского водохранилища, недалеко от станции метро «Водный стадион»: три больших новых здания компания приобрела в 2013 году за 350 миллионов долларов. За зданиями расположены два футбольных поля, несколько дорожек ведут к пляжу, по ним прогуливаются и обсуждают работу сотрудники компании. Летом неподалеку проходят соревнования по женскому волейболу, в обеденный перерыв многие берут кофе и идут на трибуны.

Когда 12 мая 2017 года по всему миру распространялся шифровальщик *WannaCry*, здания «Лаборатории» быстро опустели: на выезды к зараженным клиентам отправились даже те сотрудники, которые обычно сидят в офисах. По словам одного из сотрудников, с собой они обычно берут «специальные чемоданчики», в которых есть переходники на все разъемы, провода, «чистые» жесткие диски, энергетический батончик и банка с кофе.

Телефоны «Лаборатории» продолжали звонить, но сотрудников на всех не хватало. «Это было в пятницу, я говорил звонящим: „Давайте в субботу днем приедем“ — они отвечали: „Нам все равно, главное — чтобы в понедельник все работало“», — вспоминает Сергей Голованов.

За следующие несколько дней *WannaCry* атаковал около 200 тысяч компьютеров: железнодорожного оператора *Deutsche Bahn* в Германии, автомобильные заводы *Renault* во Франции и *Nissan* в Японии, телекоммуникационную компанию *Telefonica* в Испании, государственные больницы в Великобритании. В России вирус атаковал телефонного оператора «Мегафон» — сотрудники не могли использовать внутреннюю систему компании. Также в России вирус зашифровал компьютеры некоторых отделений полиции — из-за этого там не могли выдавать водительские удостоверения.

В связке со своим вирусом-шифровальщиком создатели *WannaCry* использовали для атаки кибероружие *EternalBlue*, созданное американским АНБ. Именно эти эксплойты позволили так быстро и успешно распространить вирус. *EternalBlue* появился в открытом доступе 14 апреля 2016 года — его выложили хакеры из группы *Shadow Brokers*. Тогда они уверяли [\[297\]](#), что смогли получить разработку того же подразделения американских спецслужб, которое разработало *Stuxnet*. Президент *Microsoft* (программа использует именно уязвимости в *Windows*) сравнил [\[298\]](#) случившееся с потенциальной кражей крылатых ракет «Томагавк».

Через месяц после *WannaCry* — в июне 2017 года — похожий на него вирус провел самую разрушительную и дорогостоящую кибератаку в истории.

*NotPetya* действовал очень просто. Вирус попадал в компьютер, работающий на *Windows*, скачивал из интернета программу и шифровал жесткий диск, блокируя к нему доступ. После этого компью-



тер показывал пользователю «синий экран смерти» с требованием выкупа: чтобы данные не были уничтожены, злоумышленники требовали перевести им 300 долларов в биткоинах. Вирус распространялся мгновенно: попав в один компьютер локальной сети, он быстро заражал все остальные.

Первыми жертвами вируса, который потом называли *NotPetya*, стали украинские компании, но атака быстро поразила весь мир — от больницы в США до шоколадной фабрики в Тасмании, в России пострадали «Роснефть» и *Evrax*. «Вся экономика у нас транснациональная, и поэтому вирус из одних офисов перетек в другие, причем за несколько минут», — объясняли в «Лаборатории Касперского». По данным журнала *Wired*, общий ущерб от вируса составил 10 миллиардов долларов.

В работе вируса *NotPetya* могла использоваться программа *Mimikatz*, написанная французским программистом Бенджаменом Делфи. Делфи вспоминал [299], что в 2013 году он выступал с презентацией программы на конференции по компьютерной безопасности в Москве и однажды, когда вернулся в свой отель, обнаружил в своем номере мужчину в черной одежде, стоявшего у включенного ноутбука француза. Мужчина пытался войти в систему; увидев хозяина комнаты, он пробормотал, что перепутал комнату и что, видимо, ключ от его номера случайно подошел к номеру Делфи, — и ушел.

Спецслужбы США и Великобритании заявляли [300], что за вирусом *NotPetya* стояли российские военные из ГРУ. Изначальной целью атаки, видимо, была финансовая система Украины.

Заместитель секретаря Совбеза РФ Олег Храмов говорил [301], что российская критическая инфраструктура никак не пострадала из-за *WannaCry* и *NotPetya* благодаря ГосСОПКА. Впрочем, специалисты уверены, что это не последняя атака.

«Это эхо, демоверсия будущей масштабной кибервойны, — указано в отчете [302] *Group-IB* о *WannaCry*. — Стало понятно, насколько уязвим современный мир перед цифровым оружием из арсенала спецслужб и киберармий, когда оно оказывается не в тех руках. К сожалению, вся история человечества показывает, что военные постоянно живут в ожидании новой войны: наличие внешнего врага позволяет раздувать бюджеты и получать звезды на погоны. Штука в том, что при современном развитии технологий любая война, в том числе и в киберпространстве, для человечества может оказаться последней».

\*\*\*

Илья Сачков — один из немногих экспертов, согласившихся под собственным именем поговорить с мной о российских хакерах и их возможных связях с государством. Сачков создал компанию *Group-IB*. В начале октября 2016 года Сачков организовал в Москве конференцию, на которой присутствовали как представители Интерпола, так и сотрудники ФСБ и управления «К» МВД; после того как хакеры



стали одной из главных тем для СМИ, Сачков стал постоянным героем глянцевого журналов и нанял себе охрану.

Офис *Group-IB* занимает несколько этажей в здании неподалеку от центра Москвы. В комнате расследователей стены завешаны символикой интернет-активистов *Anonymous*, в кабинете Сачкова на стене — благодарности за помощь от ФСБ и от МВД. Сачкову около тридцати, он закончил кафедру информационной безопасности МГТУ имени Баумана; по офису он ходит с блокнотом с наклейкой российского пропагандистского сайта *Sputnik*, на которой выведено: «*Telling the Untold*» («Рассказывая нерассказанное». — Прим. Авт.).

По его мнению, в мире «идет кибервойна» и государству «глупо не создавать киберкомандования и научные роты» (см. главу 25). Сачков рассказывает, что Минобороны, видимо, сталкивается и столкнется с проблемой поиска нужных специалистов: «безопасников» нанимают и интернет-гиганты, и банки, и коммерческие расследователи киберпреступлений.

«После окончания холодной войны история шпионажа не закончилась, — рассуждает Сачков. — В России есть Служба внешней разведки, задача которой — добывать информацию. Ни для кого не секрет, что наиболее эффективный способ это сделать — это технологии».

Впрочем, Сачков надеется, что с хакерскими группировками российское государство не сотрудничает. По его мнению, хакеров можно контролировать, только если посадить их в комнату, наставить на них автоматы Калашникова или мотивировать их страхом: либо тюрьма, либо выполнение задач. Он уверен, что кибероружие в самое ближайшее время может выйти из-под контроля: удары будут нанесены не по сайтам или личной переписке, а по более серьезным объектам, например по критической инфраструктуре страны или по ее финансовой системе.

«Обычно [хакерские] группы, когда замечают, что их отследили, полностью меняют структуру [своих атак]. *Fancy Bear* совершили ряд резонансных взломов, но при этом несложно эти атаки увязать между собой: они действуют по одному алгоритму, — рассуждает Сачков. — Они [*Fancy Bear*] — либо идиоты, либо не боятся».

— То есть они уверены в собственной безнаказанности?

— Да.



## Глава 35

### За нами следят

В мае 2016 года Роман Удот убедился, что его телефон прослушивают.

Удот давно работает в ассоциации наблюдателей «Голос», которая отслеживает нарушения на выборах (и крайне нервирует российские власти). «Если ты представляешь интерес, твой телефон прослушивают, это как дважды два — четыре, — говорит он. — Узнают из разговора, куда я хожу ужинать с друзьями? Это издержки того, чем мы занимаемся. С этим нужно смириться».

В последнее время на многих встречах и мероприятиях «Голоса», о которых не сообщалось публично, появлялись сотрудники телеканала НТВ — из отдела, снимающего сенсационные «разоблачительные» фильмы, посвященные российским оппозиционерам (фильм о «Голосе» [вышел](#) 3 июня 2016 года).

Тогда Удот и его коллеги решили поставить эксперимент. Как-то раз с «Голосом» по электронной почте связались представители канадского посольства. Они попросили о встрече, чтобы обсудить грядущие думские выборы и работу ассоциации. Обычно такие встречи проходили в посольстве или в кафе, но в этот раз дипломаты предложили встретиться в офисе наблюдателей. Точные договоренности по месту и времени обсуждали исключительно по телефону — чтобы проверить, появятся ли после этого на встрече сотрудники НТВ.

Когда канадцы приехали в офис, возле здания почти сразу же появился автомобиль телекомпании. В разговоре с Удотом сотрудники НТВ сказали, что не прослушивают его телефон. Через несколько дней в этих же людях бывший посол США в России Майкл Макфол [узнал](#) тех, кто в 2012 году появлялся вместе с ним на мероприятиях, проведение которых никак не анонсировалось. Госдепартамент США тогда [предполагал](#), что телекомпания получила доступ к календарю посла, взломав почту или телефоны.

Специалист по информационной безопасности одной из российских компаний, занимающихся киберзащитой, рассказывал мне, что в случае Удота речь может идти о слежке спецслужб через СОРМ (аппаратура для прослушки, которой оперативники ФСБ пользуются по решению суда) или вирусе-шпионе в телефоне. Есть, однако, и еще один вариант — прослушка могла осуществляться через уязвимость в мобильной связи, о которой знают только специалисты по информационной безопасности и операторы связи: «дыру» в системе протоколов SS7, используемой телефонными компаниями для передачи служебных команд. Благодаря этой уязвимости после несложного взлома можно перехватывать и прослушивать звонки, отслеживать местонахождение абонента, читать и даже переписывать SMS.

Под ударом может оказаться практически любой обладатель телефона — политик, правозащитник, журналист, бизнесмен, жена ревнивого мужа, муж ревливой жены; прочие семь с половиной милли-



ардов абонентов мобильных телефонов. Хакеры могут атаковать любые телефоны — и старые кнопочные, и смартфоны, и устройства на базе *iOS* или *Android*.

От атак через SS7 не защищены около 90 % мобильных операторов мира (в безопасности находятся операторы, заменившие устаревшие протоколы и те, которые постоянно анализируют всех абонентов для выявления вредоносных действий); SMS-сообщения 89 % абонентов можно перехватить; 58 % абонентов можно отследить; разговоры половины абонентов можно прослушать. Об этом говорится в докладе российской компании *Positive Technologies*, исследовавшей системы безопасности крупнейших мобильных операторов мира.

\*\*\*

Протоколы SS7 начали разрабатывать в 1970-х годах. В то время радиолюбители увлекались конструированием самодельных аппаратов, с помощью которых удавалось имитировать передачу сигналов между телефонными станциями («межстанционную сигнализацию») и отправлять на них нужные команды. Такие аппараты, известные как «синие коробки», позволяли звонить почти бесплатно по любым направлениям, оплачивая звонки как местные. «Синюю коробку» в своем гараже собрали, например, создатели *Apple* Стив Джобс и Стивен Возняк.

Для борьбы с мошенниками телефонные компании разделили абонентский (передачу голоса) и служебный трафик (технические команды). Так появилась SS7, система сигнальных протоколов для обмена информацией и маршрутизации вызовов (какой номер вызывает, кого, откуда и так далее). Ее можно сравнить с системой метрополитена: SS7 — это служебные тоннели для рабочих, а не те, по которым ходят поезда.

SS7 начала работать в начале 1980-х и объединила телефонных операторов по всему миру. В России, США, Азии и Европе протоколы называются по-разному, они незначительно различаются, но совместимы друг с другом; в целом система по своему устройству напоминает интернет. В России SS7 называют ОКС-7 (общий канал сигнализации № 7), в США — CCS7, в Германии — N7, в Великобритании — CCIS7; общепринятое название — SS7.

В начале 2000-х годов было разработано дополнение к SS7 — программное обеспечение *Sigtran*, которое позволило передавать сообщения и команды по IP-сетям: компоненты сети SS7 стали доступны в публичных сетях, подключиться к некоторым из них можно через интернет. Новое и инновационное ПО продолжило работать на старой системе, которую никак не защитили; более того, осуществить «врезку» в эту систему теперь оказалось даже проще.

Публичное обсуждение «дыры» в SS7 началось в 2008 году. На хакерской конференции *Chaos Computer Club* (одна из крупнейших в мире) немецкий исследователь информационной безопасности То-



биас Энгель показал [\[303\]](#) собравшимся способы слежки за абонентами мобильной связи, основанные на проникновении в SS7. В правительствах и спецслужбах об уязвимости, видимо, знали еще раньше. В книге специалистов по телекоммуникациям Томаса Портера и Майкла Гуфа, вышедшей в 2007-м, указывалось, что администрация президента США серьезно обеспокоена высоким уровнем угрозы атак на основе SS7; в других американских документах [\[304\]](#) такие атаки упоминались еще с 1998 года. Об уязвимости не могли не знать мобильные операторы, но они, как правило, отказываются признавать существование проблемы.

В 2013-м бывший сотрудник ЦРУ и Агентства национальной безопасности США Эдвард Сноуден передал журналистам *The Guardian* и *The Washington Post* архивы, подтверждающие, что спецслужбы США и Великобритании сами могут следить за любым человеком на планете (и пользуются этой возможностью). В том же году *The Washington Post* рассказала [\[305\]](#), что АНБ использовала «дыры» в SS7 как один из методов слежки. А еще через год журналисты издания сообщили [\[306\]](#) о специальных программах для слежки на основе SS7 и том, что с помощью SS7 хакеры могут [\[307\]](#) «определить местоположение абонента в любой точке мира, прослушивать разговоры в реальном времени или записывать зашифрованные звонки и текстовые сообщения для дальнейшей расшифровки».

В первые годы к SS7 имели доступ избранные коммерческие и государственные телефонные компании. В конце 2010-х подсчитать количество легальных подключений к SS7 невозможно: это и мобильные операторы, и виртуальные мобильные операторы, и развлекательные контент-провайдеры. В этих компаниях работают сотни тысяч человек; среди них могут оказаться и нелояльные сотрудники с необходимыми навыками.

\*\*\*

В 2014 году российские специалисты по кибербезопасности Дмитрий Курбатов и его коллега Сергей Пузанков проверили, насколько легко найти оператора, готового подключить незнакомцев к SS7. Беседуя с представителями мобильных операторов из Южной Америки и Средней Азии, они прикинулись начинающими контент-провайдерами дополнительных услуг, которым требуется подключение к SS7, чтобы «рассылать абонентам лучшие прогнозы погоды». Многие операторы согласились дать им доступ официально, другие предлагали подключение за четыре тысячи долларов. По словам Курбатова, имея знакомых в любом из операторов связи, получить доступ к SS7 очень легко.

Для атаки на абонентов не требуется сложное оборудование. «Не нужно быть гением или службой разведки, чтобы все это реализовать, — говорит Курбатов. — Программный комплекс мы сами написали, дополнив скачанное из интернета. Порог входа — низкий».



Достаточно с помощью соответствующего софта узнать номер IMSI — специальный идентификатор, который присваивается каждому мобильному абоненту (содержит код страны, код оператора и внутренний уникальный номер сим-карты). Одновременно хакер получает параметры MSC / VLR (коммутатор вызовов и местоположения), благодаря которым абонент находится в сети.

Все это требуется, чтобы обмануть «домашнюю» сеть абонента и перевести его в свою — фальшивую. Для «домашней» сети это будет выглядеть так, будто абонент («цель») уехал в роуминг; сам абонент об этом никогда не узнает. Фальшивая сеть передаст команду оператору, что теперь сама обслуживает абонента (то есть оператор получит сигнал, что его абонент находится в зоне обслуживания другого мобильного оператора). После этого с помощью специального ПО хакер сможет перехватить SMS, прослушать звонки, отследить местоположение «цели».

Курбатов говорит, что такой доступ в меньшей степени используется для слежки; чаще — для воровства денег с мобильных кошельков и SMS-банкинга: это обычно небольшие деньги, но преступные группировки берут оборотом [\[308\]](#).

Получив доступ к SS7, хакер может перехватить [\[309\]](#) коды авторизации от *Telegram*, *WhatsApp* и пароли двухфакторной авторизации *Gmail*, *Facebook*, «ВКонтакте». Инициировав подключение к *Telegram*, злоумышленник может получить SMS с паролем на захваченный телефон, ввести его и получить полноценный доступ к мессенджеру — писать сообщения от лица абонента и прочитать всю его переписку, которую *Telegram* автоматически подгружает в новый телефон; закрытыми для чтения останутся только зашифрованные чаты. В *WhatsApp* старую переписку прочитать не удастся: она не хранится на сервере, с апреля 2016 года *WhatsApp* включил полное шифрование для всех пользователей.

«Все, что зависит от SMS, может быть взломано — и было уже взломано с момента, когда заработала SS7, — говорил [\[310\]](#) немецкий хакер Карстен Нол. — Мобильная сеть, видимо, самое слабое звено в нашей цифровой защите».

Жертвы редко узнают, что их взломали. Согласно исследованию [\[311\]](#) американской компании *FireEye*, занимающейся разработкой программ от кибератак, среднее время нахождения хакера во взломанной сети или аккаунте до обнаружения — 205 дней.

В ночь на 29 апреля 2016 года о взломе своих аккаунтов в *Telegram* сообщили [\[312\]](#) оппозиционер Олег Козловский и сотрудник Фонда борьбы с коррупцией Георгий Албуров, оба — абоненты МТС. Неизвестные перехватили SMS с авторизационными кодами от их аккаунтов. Этого было достаточно, чтобы войти в систему, — у оппозиционеров не была включена двухфакторная авторизация с паролем. Козловскому и Албурову SMS с авторизацией не пришли. Козловский рассказывал, что в момент взлома МТС отключил службу доставки SMS.



В службе поддержки ему якобы заявили [\[313\]](#): «Услугу коротких сообщений вам отключил наш отдел технической безопасности». Позже активисты выложили квитанции за услуги за апрель 2016 года: и у Козловского, и Албунова в них указано отключение услуг коротких сообщений. МТС это опровергал, представитель МТС Дмитрий Солодовников сообщил [\[314\]](#): «Никаких целенаправленных действий по отключению услуг не производилось. Не исключая вероятности вирусной атаки или доступа к аккаунту через веб-интерфейс». Таким же образом, возможно, прослушивали заместителя госсекретаря США Викторию Нуланд с послом США в Киеве Джеффри Пайеттом — тогда неизвестные выложили запись их телефонного разговора. Первым ссылку на аудиозапись тогда выложил помощник Дмитрия Рогозина, вице-преьера по обороне в правительстве.

Если оппозиционеров атаковали через SS7, хакеры вполне могли сделать так, чтобы взломанным абонентам не пришло SMS.

Помимо перехвата звонков и сообщений с помощью атак через SS7, хакер сможет вывести телефон из строя: устройство показывает, что ловит сигнал, но до него нельзя дозвониться. Такие атаки могут навредить бизнесменам во время переговоров, журналистам, связывающимся с источниками. Они также могут использоваться во время вооруженных конфликтов.

Российские спецслужбы давно занимаются созданием вирусов-шпионов, которые подсаживаются на телефоны — обычно для этого нужен физический контакт с устройством. Впрочем, есть у них и другие способы слежки, не требующие сложных ухищрений: например, они могут использовать COPM, систему технических средств для обеспечения оперативно-розыскных мероприятий, которая позволяет в том числе следить за телефонными переговорами или интернет-трафиком. По российскому законодательству спецслужбы имеют право задействовать систему только по решению суда, однако в 2012 году Верховный суд России признал законным [\[315\]](#) право спецслужб прослушивать оппозиционеров только на основании того, что они занимаются протестной деятельностью. В расследовании [\[316\]](#) российского *Forbes* указывалось, что решение о прослушке сотрудник ФСБ никому показывать не обязан: операторы связи не имеют права знать, чьи переговоры или почту перехватывают спецслужбы. Пункты управления COPM соединены по защищенному кабелю с серверами мобильных операторов и интернет-провайдеров, для прослушки сотруднику ФСБ достаточно ввести команды на пульте управления COPM, который находится в здании местного управления ведомства.



## Глава 36

### Анонимы против государства

4 марта 2018 неизвестные взломали сайт Государственного ракетного центра имени академика В. П. Макеева — производителя «непредсказуемых ракет», которыми Владимир Путин хвастался во время своего обращения к Федеральному собранию. Вместо привычной титульной страницы на сайте появилась картинка с изображением темнокожего мужчины в БДСМ-наряде; рядом была надпись «*putin moja raketa gotova*».

Впрочем, сайт быстро вернули в прежний вид, а продолжения взлом не имел. В последние годы «оппозиционных» хакерских атак вообще стало гораздо меньше — их расцвет пришелся на первую половину 2010-х, после чего российское государство фактически объявило нападавшим гражданскую кибервойну.

В феврале 2012 года неизвестные хакеры взломали почтовый ящик главы Росмолодежи Василия Якеменко — идеолога и создателя прокремлевских молодежных движений, которые были созданы в начале нулевых для борьбы с «оранжевой революцией» и оппозицией. Корреспонденция Якеменко была выложена в открытый доступ под хэштегом *#OpYoungBustards* в нескольких блогах: *KremlinGate*, *UltraZashkvar*, *Rumol-Leaks*. Интереснее других была переписка Якеменко с пресс-секретарем Росмолодежи Кристиной Потупчик, которая долгое время была одной из самых заметных участниц движения «Наши».

Из переписок можно было узнать, что Якеменко обсуждал со своими соратниками организацию DDoS-атак и взломы почтовых ящиков оппозиционеров. Значительная часть переписки касалась платного размещения материалов в популярных российских блогах — за них платили сотни тысяч рублей. Самым дорогим якобы было размещение постов у Ильи Варламова — около 400 тысяч рублей за два материала о посещении Путиным авиасалона МАКС-2011 и о съезде «Единой России», на котором стало известно о том, что Путин идет на третий срок. В разговоре со мной Варламов отрицал, что получил за посты деньги. Кроме того, деньги от государства получал проект «Спасибо, Ева», для которого многие видеоблогеры делали ролики. Один из них — Данила Поперечный, делавший серию пропагандистских мультфильмов про Владимира Путина, — признавался, что не знал, из каких денег ему платили зарплату.

Кроме прочего, из переписки можно было узнать про работавших на Якеменко платных комментаторов — прообраз того, что потом станет называться «фабрикой троллей» (см. главу 25). Якеменко и Потупчик решили [\[317\]](#) собрать группу людей «с подвешенным языком, хорошо пишущих, не дебилов», которые должны были «обсирать оппозицию и хвалить Путина» на форумах и в соцсетях, чтобы имитировать мнение народа». «Нужна картинка того, что за нас большинство», — поясняли в переписке. Зарплата таких сотрудников составляла от 20 до 30 тысяч рублей в месяц; точная сумма



зависела от количества удачных комментариев и дискуссий; некоторых награждали айпадами. Расходы на таких комментаторов, как было указано в одном из отчетов, составляли около 600 тысяч рублей в месяц.

В другом письме якобы Кристина Потупчик (письма были отправлены с того же адреса, который был указан в качестве личной почты в «Живом журнале» активистки) предлагала организовать DDoS-атаку на «Коммерсант», чтобы «парализовать сайт на 5 часов, создать невыносимые условия, психологически и физически доканать». В отчете, составленном для Якеменко, она указывала, что «серьезные ресурсы, которые нельзя полностью ликвидировать, периодические подвергаются активным DDoS-атакам».

В одной из смет отдельно фигурировал некий Арсен Мухматмурзиев — его сфера полномочий характеризовалась как «ИТ-специалист, хакер, выведение из строя ресурсов противников, взлом сайтов, взлом аккаунтов»; платили ему 40 тысяч рублей в месяц. Другой активист в письме главе Росмолодежи предлагал услуги «спаминга и троллинга ведущих блогеров, которые публикуют антигосударственные записи», DDoS-атак и вывода из строя «даже самых защищенных ресурсов», требуя за них 18 миллионов рублей в год.

Кристина Потупчик сейчас ведет блог о книгах и позиционирует себя как гражданскую активистку. Василий Якеменко сначала открыл кафе «Ешь пирог», потом занялся [\[318\]](#) книжным клубом и купил [\[319\]](#) дом в Баварии. Другие участники операций Росмолодежи заняли околосударственные должности в разных российских регионах. Методы борьбы с оппонентами, которые они опробовали в России, через несколько лет начали использоваться на выборах в США и европейских странах.

\*\*\*

В апреле 2014 года один из руководителей организации, занимающейся прокремлевскими ботами, назначил [\[320\]](#) мне встречу в любимом месте выходцев из движения «Наши» — баре неподалеку от метро «Сухаревская».

Он начал заниматься информационными войнами в декабре 2011 года — после массовых оппозиционных протестов. Сначала его работа заключалась в том, чтобы руководить группой «мурзилков» — журналистов и блогеров, которые за определенную плату отрабатывали нужную Кремлю повестку, при этом не показывая в лоб, что они работают на власть. По его словам, каждый день он рассылал «мурзилкам» брифы, полученные из администрации президента, — документы, в которых указывалось, как и с какими акцентами освещать события.

Некоторых партнеров он находил в кафе, популярных у интеллигенции. «Приходишь, смотришь: кто-то, может, в деньгах нуждается, кто-то, может, не совсем ярый оппозиционер, — рассказывал он. —



Выцепляли кого-то, предлагали попробовать: тысяч за пятнадцать написать про какого-нибудь проворовавшегося главу управы Биби-рево. Человек думал примерно так: благое дело, еще и денег получу, девочку в „Жан-Жак“ свожу. И так ты ему раз, два, а на третий говоришь: „Напиши-ка про Навального“. Он отказывается. Говоришь: „Ха, ты хочешь, чтобы все узнали, что ты уже брал деньги?“»

По словам моего собеседника, после взлома почты Кристины Потупчик все стали действовать аккуратнее: регистрировали секретные ящики или даже, чувствуя себя супершпионами, проверяли, нет ли за ними слежки, при встречах с коллегами по бизнесу.

Все деньги он получал наличными и мог распоряжаться ими по своему усмотрению: снимать офис, нанимать людей. Кроме его организации, похожими вещами в Москве 2014 года занимались еще 7 организаций. На общих собраниях они в том числе обсуждали, кому заказать DDoS-атаки на оппозиционные сайты и кого нанять для накрутки просмотров и лайков у прогосударственных видеороликов и твитов. Для этого, например, использовались фишинговые приложения вроде «Узнай свой психологический возраст», с помощью которых можно было получить доступ к аккаунтам и использовать их для ретвитов.

В конце разговора собеседник, усмехнувшись, сказал, что, учитывая последние успехи Путина (имелись в виду Олимпиада в Сочи и присоединение Крыма), скоро может остаться без работы. «В информационных войнах мы всех переиграли», — уверенно заявил он. Он ошибался. Если в России помощь ботов и хакеров больше почти не требовалась, то в мировом масштабе в следующие годы их атаки начали учащаться с невероятной скоростью.

\*\*\*

В феврале 2012 года хакеры, взломавшие Василия Якеменко и других чиновников, согласились [\[321\]](#) пообщаться со мной в зашифрованном чате. Себя они назвали российским подразделением *Anonymus* — международного движения киберактивистов, которые с 2008 года начали проводить атаки на корпорации, кино- и звукозаписывающие компании под лозунгами свободы распространения информации. Люди, ассоциировавшие себя с *Anonymus*, активно участвовали в так называемой Арабской весне — волне революций, прокатившейся по нескольким странам Ближнего Востока в начале 2010-х годов. В России переписками госслужащих и прокремлевских активистов их деятельность не ограничилась — хакеры также взломали [\[322\]](#) сайт калужского отделения «Единой России» и разместили на нем видеоролик, в котором обещали чиновникам постоянную слежку и хвастались тем, что найти их невозможно: хакером может быть «ваш бухгалтер, почтальон, секретарь, адвокат, даже ваш сын».

«Единственное, что все мы разделяем, — это стремление защитить свободу слова в интернете, — писал мне один из хакеров. — Не наступит день, когда аноним позволит кому-либо подменять его



мысли». Он объяснял, что кремлевских чиновников они взламывали, в частности, в отместку за взлом почты Алексея Навального, осуществленный «хакером Хэллом» (см. главу 22).

В марте 2012 года «анонимы» организовали DDoS-атаку на сайт телеканала НТВ, где вышел пропагандистский фильм «Анатомия протеста» (в нем сообщалось, что участники оппозиционных митингов получали деньги за участие в акциях). Сайт НТВ не работал 12 часов.

6 мая 2012 года — во время оппозиционного митинга на Болотной площади, закончившегося столкновениями с полицией и уголовными делами против рядовых протестующих — «анонимы» призвали сторонников атаковать сайты президента и правительства. Для новичков они выложили подробные инструкции, как действовать, и ссылки на нужные программы. «Мы поддержим этот протест отключением лживых государственных сайтов — и в первую очередь сайта правительства Российской Федерации... Всего несколько простых действий приблизят прогнившую коррумпированную систему к закономерной гибели. Она разрушит себя сама», — заявляли они в своем обращении. Своей цели они достигли: государственные сайты — в том числе сайт президента — ненадолго перестали открываться.

Пока одни спецслужбы заводили «Болотное дело» против участников митингов, другие начали искать тех, кто протестовал в интернете. Уже через месяц сотрудники ФСБ в Красноярске задержали двадцатилетнего студента колледжа радиоэлектроники Павла Спасского и бывшего чиновника Василия Никитина; в Томске задержали менеджера местной мелкой фирмы Сергея Тюлюпова. Все они были новичками, которые ничего не понимали в хакинге. Следуя инструкциям *Anonymous*, они скачали нужные программы и настроили их для DDoS-атак. Все в итоге получили [323] сроки: Спасского приговорили к двум годам условно и штрафу в 25 тысяч рублей, Никитин отсидел год, Тюлюпов — полтора.

Впрочем, «анонимов» это не остановило. В июне 2013 года они начали атаковать сайты Роскомнадзора — ведомства, которое отвечает за контроль над интернетом. Параллельно активисты опубликовали [324] в «Ютьюбе» обращение к россиянам. Как и их зарубежные коллеги, российские хакеры выкладывали в «Ютьюб» обращения с измененным голосом, во всех роликах присутствовала маска Гая Фокса — символ борьбы с репрессивными правительствами:

Много лет вы подвергаетесь унижениям и показным издевательствам в своей собственной стране, отдавая все и ничего получая взамен. Правовой и законодательный беспредел, коррупция и вдобавок — непрерывный поток лживой пропаганды, льющийся на вас из телевизора, привели к тому, что многие люди принимают это как должное и не представляют своей жизни иначе, а сопротивляющиеся подвергаются гонениям.

Однако есть место, где пока еще гражданам России не получается промывать мозги. Это интернет. Здесь человек



всегда может найти единомышленников, узнать информацию, не подвергнутую цензуре, из первых рук и сделать выводы. Самостоятельно. Но под прикрытием заботы о детях и борьбы с пиратством, а на самом деле с целью установления тотальной цензуры над сетью интернет и из желания получать больше денег, развернута кампания по контролю над сетью. Вместо настоящих новостей вы будете видеть ту же ложь, что и на «Первом канале», отдавать из вашей небольшой зарплаты на подделки, которые вам преподносят как «искусство». Тот, кто захочет попасть в свободный интернет, будет вынужден «нарушить» закон и, вполне вероятно, окажется в тюрьме.

Если вы позволите забрать у вас интернет, то больше никогда не получите его назад. Протестуйте против любых законов, покушающихся на вашу свободу в сети, не позволяйте ограничивать свободный обмен информацией и не верьте в лживые заявления об опасности мировой паутины. А всем ответственным за эти действия необходимо понять, что попытки установить в сети свой контроль и повлиять на интернет-сообщество, не будут смиренно приняты. На каждый закрытый вами сайт мы взломаем два, на каждую вашу ложь мы ответим разоблачающей правдой, на каждую вашу меру мы найдем контрмеры. Мы – Анонимы, и имя нам – легион. Мы не прощаем, мы не забываем.

Предостережения «анонимов» оказались точными, но защитить интернет им так и не удалось: в последние годы российские власти последовательно ограничивают его свободу.

\*\*\*

Ведомство, которое отвечает за контроль над интернетом, — Роскомнадзор — располагается в восьмиэтажном здании [\[325\]](#) на Китай-городе, отделанном серой плиткой и окруженном голубыми елями; там же сидит Министерство культуры. До администрации президента от Роскомнадзора — пять минут медленным шагом.

До осени 2012 года о деятельности ведомства знали только профильные специалисты. Роскомнадзор появился в 2008 году — подразделение «откололось» от Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия. В его полномочия попали надзор за СМИ (в том числе выдача предупреждений о нарушениях — издание, получившее два и больше предупреждений, может быть закрыто) и связью: оформление лицензий на радиочастоты, выдача разрешений на судовые радиостанции и на строительство линий связи.

По-настоящему прославился Роскомнадзор после того, как в 2012 году приняли поправки в закон «О защите детей от информации, причиняющей вред их здоровью и развитию» — его еще называли «законом о черных списках». Главным нововведением стал «Единый реестр доменных имен, указателей страниц», то есть спи-



ми надзорных органов. Реестр создавался для операторов связи, которые должны блокировать для своих клиентов доступ к попавшим в список сайтам. Одним из инициаторов поправок выступала Елена Мизулина, депутат Госдумы, прославившаяся законом о «запрете гей-пропаганды».

На этом репрессивные меры в отношении интернета не закончились. 22 апреля 2014 года в почту сотрудника администрации президента Тимура Прокопенко упало сообщение от близкого к Кремлю политолога Дмитрия Бадовского (почту Прокопенко впоследствии взломали и опубликовали в интернете). К письму был приложен файл под названием «интернет\_короткое предложение». В тексте говорилось: «Контроль над Интернетом до сих пор официально принадлежит США», потому что у них в руках «система тотальной слежки АНБ». Политолог предлагал «разработать и принять... закон, обязывающий зарубежные интернет-компании организовать полную обработку данных российских пользователей исключительно на территории России».

Уже через два месяца этот закон внесли [\[326\]](#) в Госдуму — и быстро приняли. Теперь все сервисы, обрабатывающие персональные данные граждан России, обязаны хранить их на серверах, расположенных в России.

В феврале 2017 года был принят «пакет Яровой», который в том числе обязал [\[327\]](#) хранить все записи звонков и любые сообщения, которыми обмениваются пользователи, в течение полугода. В течение трех лет провайдеры и мессенджеры должны хранить метаданные — то есть не само содержание разговоров и переписки, а сведения о том, что такой-то разговор или такой-то обмен смс-сообщениями состоялся такого-то числа в таком-то часу. Эти же правила действуют и для «организаторов распространения информации в сети Интернет» (к ним относятся интернет-ресурсы, внесенные в соответствующий реестр) — только срок хранения метаданных в их случае составляет не три года, а один.

К 2017 году Роскомнадзор каждый день в среднем блокировал [\[328\]](#) 244 страницы в интернете, а каждые восемь дней суды приговаривали к реальному сроку людей, которых обвиняли в экстремизме по 282 статье УК РФ — каждый год по ней в тюрьмы попадали больше 500 человек (в конце 2018 года их перестали возбуждать после декриминализации статьи). За последние пять лет Роскомнадзор заблокировал более 10 миллионов сайтов.

Активность «анонимов» тем временем почти сошла на нет. Последние атаки они провели весной 2014 года. В марте 2014-го *Anonymouse* в ответ на увольнение главного редактора lenta.ru атаковали сайт Кремля, некоторое время он оказался недоступен. В твиттере они написали [\[329\]](#): «Сайт Кремля взъебан». Вскоре они же атаковали сайты МИДа, «Первого канала», «Российской газеты». Когда сайты переставали открываться, они радовались и писали в твиттере: «*Tango down!*»



В 2015 году несколько твиттеров активистов были взломаны; а в 2016 году на одном из их ютьюб-каналов начали выкладывать видео от имени группировки *Fancy Bear* — прогосударственных российских хакеров. Они рассказывали [\[330\]](#) о взломе антидопингового агентства WADA, обвиняли американских спортсменов во лжи и заявляли, что будут добиваться чистоты в международном спорте.



## Глава 37

### Бангкокский связной

14 августа 2014 года около десяти утра неприметный мужчина зашел в кафе в районе Тишинской площади в Москве. Он заказал кофе, устроился в дальнем углу заведения, открыл недорогой нетбук и запустил несколько программ: текстовый редактор, зашифрованный чат и браузер. Потом он подключился к бесплатному вайфаю и вышел в интернет через VPN на собственном сервере — так, чтобы отследить его действия было невозможно. Открыл в браузере твиттер, ввел логин и пароль, которые были сохранены в отдельном документе, и написал первый твит: «Ухожу в отставку. Стыдно за действия правительства. Простите».

Запись появилась в официальном аккаунте премьер-министра России Дмитрия Медведева. Ее увидели два с половиной миллиона подписчиков.

Попивая кофе, мужчина написал еще несколько твитов: «Стану свободным фотографом. Давно мечтал»; «Несмотря на наши инициативы, неким сетевым хулиганам ср@ть на доступ в сеть по паспорту ( ((»; «Давно хотел сказать. Вова! Ты не прав!»; «Мне нравится читать @navalny». Затем ретвитнул бывшего главу предвыборного штаба Алексея Навального Леонида Волкова и оппозиционного журналиста Романа Доброхотова. Наконец написал: «Вы думаете, в Ялте сегодня скажут что-то важное? Сомневаюсь. Вот сижу тут, а сам думаю, а на х\*я?»

Мужчине не казалось, что он делает что-то экстраординарное. Он вообще поначалу не собирался идти в это кафе и писать в аккаунт премьер-министра — просто больше было некому. В тот день он оказался единственным не занятым на основной работе человеком из группировки «Анонимный интернационал», широко известной как «Шалтай-Болтай». Хакеры из «Шалтая» получили ключи от твиттера премьера уже давно, когда выкачали из *iCloud* электронные копии трех смартфонов Медведева: пароли от соцсети премьер хранил в заметках на айфоне. Взлом твиттера группировка приурочила к ялтинской речи Владимира Путина. В Крыму, уже присоединенном к России, президент выступал с речью перед правительством и парламентом.

«Мы следили за Медведевым два года, но ничего интересного не попадалось, поэтому решили просто потроллить», — так мне объяснил смысл взлома один из членов «Анонимного интернационала».

Спустя полчаса после первого твита пресс-секретарь президента России Дмитрий Песков заявил информагентствам: «С большой долей вероятности могу предположить, что это проявление хакерства». В правительстве подтвердили: твиттер премьера взломали. Последние сообщения, размещенные в микроблоге, не соответствуют действительности». Сотрудники пресс-службы премьер-министра удалили несколько опубликованных твитов, однако мужчина из кафе успел написать еще кое-что: «Мы можем вернуться в



80-е годы. Это печально. Если цель моих коллег в Кремле в этом, то она скоро будет достигнута»; «Россияне не должны страдать из-за проблем в восприятии здравого смысла у верховного руководства страны».

На прощание он ретвитнул аккаунт «Анонимного интернационала» — @b0ltai: «Цирк закончился клоуны разбежались. Запрещайте электричество»).

«Творческий техник», как в «Анонимном интернационале» называют человека, писавшего в твиттер Медведева, мог бы строчить твиты столько, сколько ему заблагорассудится: выкинуть его из соц-сети никто бы не смог. Пресс-служба, чтобы остановить происходящее, должна была попросить администрацию сервиса заблокировать аккаунт Медведева. Впрочем, спустя час мужчина написал коллегам в чат: «Скучно, я сваливаю», закрыл нетбук и вышел из кафе.

\*\*\*

«Шалтай-Болтай» — последний успешный проект российского киберсопротивления. Впервые они заявили о себе 31 декабря 2013 года, опубликовав текст новогоднего обращения Владимира Путина за несколько часов до того, как оно вышло в эфир. Следующие 12 месяцев «Анонимный интернационал» выкладывал в основном переписку, выкачанную из электронных ящиков и телефонов российских политиков разной степени влиятельности. В конце они всегда подписывались: «Всегда с Вами, даже тогда, когда Вы об этом не подозреваете».

Весной 2014-го «Шалтай» слил в сеть сценарий московского митинга в поддержку присоединения Крыма к России, документы о том, как администрация президента готовила референдум на полуострове, и предположительную личную переписку Игоря Стрелкова-Гиркина, бывшего сотрудника ФСБ, который в тот момент вместе со своими сторонниками вел боевые действия на востоке Украины. А еще — документы [331] о том, как компания Евгения Пригожина «Конкорд» курирует кремлевских «интернет-троллей» через «Агентство интернет-исследований» (подробнее о «фабрике» см. в главе 25).

Игорь Осадчий (он упоминался в переписке «Агентства интернет-исследований» как руководитель проекта «Переводчик», ответственного за размещение сообщений в зарубежных СМИ) обнаружил в публикациях свои персональные данные и подал в суд. Представитель Роскомнадзора тогда сообщил: «Суд вынес определение, что информация должна быть удалена, но хостинг-провайдер на наше уведомление не отреагировал, поэтому служба отправила операторам связи предписание о блокировке блога». 27 июля 2014 года доступ к ресурсу b0ltai.org из России был заблокирован по требованию Роскомнадзора; вскоре та же участь постигла основной твиттер группировки. Был заблокирован и основной твиттер группировки @b0ltai. Сейчас «Шалтай-Болтай» доступен в РФ только через



VPN или зеркальный сайт [332]; запасной твиттер @b0ltai2 дублирует все записи из заблокированного — вплоть до ретвитов.

За несколько дней до блокировки интернет-активисты выложили [333] предполагаемую переписку вице-премьера Аркадия Дворковича: он требовал изменить параметры бюджета на 2015-2017 годы, иначе «будет невозможно обеспечить решение большинства задач, поставленных в программных документах». Через месяц «Анонимный интернационал» рассказал [334] о трех почтовых ящиках Дмитрия Медведева и показал переписку депутата «Единой России» Роберта Шлегеля об организации атак «троллей» на сайты крупнейших зарубежных СМИ (*The New York Times*, CNN, BBC, *USA Today*, *The Huffington Post*).

Осенью 2014-го «Шалтай» слил [335] электронную переписку аффилированной с московским правительством компании «Московские информационные технологии» с российскими СМИ («Комсомольская правда», «Известия», «Российская газета», «Литературная газета», *Regnum*) — так чиновники размещали в прессе заказные статьи. Также была опубликована предполагаемая переписка [336] замначальника секретариата первого вице-премьера Игоря Шувалова. В декабре 2014-го «Анонимный интернационал» выложил фотографию, на которой бывшая пресс-секретарь движения «Наши» Кристина Потупчик сидит, предположительно, в кабинете в администрации президента с сумкой, набитой деньгами [337].

Через две недели активисты слили предполагаемую переписку заместителя начальника управления внутренней политики администрации президента Тимура Прокопенко. В своей почте он обсуждал заказные материалы [338] против Алексея Навального, по SMS общался с Алексеем Гореславским, который в тот момент работал заместителем директора по внешним коммуникациям крупного российского интернет-холдинга *Rambler&Co* (в его состав входили два самых популярных интернет-СМИ в стране: «Лента.ру», где я тогда работал, и «Газета.ру»):

– Слушай, а они тебя вообще не слушают чтоль? – интересовался Прокопенко.

– Я им всем не начальник, это во-первых. Я могу очень сильно рекомендовать, но уволить и оштрафовать не могу. В Газете слушаются, но редакция не до конца отдрочена, поэтому есть косяки. В Ленте своя позиция на все, Галя (Тимченко, главный редактор издания. — Прим. Авт.) ссылается на то, что у нее такой «стандарт» и она его будет исполнять. Вопрос перед акционером поставлен. Делаю, что могу.

Через 20 дней после этого сообщения главного редактора «Ленты.ру» Галину Тимченко уволили; вслед за ней ушла почти вся команда издания — включая меня.

По сообщениям и письмам Прокопенко вообще было хорошо понятно, как работает управление внутренней политики администрации президента России. Например, предполагаемые сотрудники президента России отслеживали каждый шаг оппозиционера Алек-



сея Навального в интернете, готовили записки о редакционной политике независимых изданий, изучали твиты и демотиваторы в социальных сетях. Прокопенко каждый день получал многостраничные доклады о главных темах, обсуждаемых в *Twitter*, *Facebook* и «Живом журнале». Каждый отчет заканчивался рекомендациями о том, как следует освещать эти темы. Например, такими: «Тему с инвалидом, которая живет в гараже из-за бездействия чиновников, может взять на себя ОНФ (Общероссийский народный фронт, созданный в 2011 году для противодействия оппозиции и поддержки Владимира Путина. — Прим. Авт.), обеспечив женщину необходимой информационно-юридической поддержкой для решения жилищной проблемы и наказания виновных в ней чиновников».

Прокопенко много общался с руководством Роскомнадзора о блокировках неугодных сайтов. В разговоре с главой ведомства Жаровым он обсуждал блокировки группы украинских националистов «ВКонтакте»: Жаров жаловался, что тогдашний глава «ВКонтакте» Павел Дуров «дурку включил, не дает дальше блокировать»; Прокопенко предлагал задействовать Генпрокуратуру и «дожать» (через некоторое время Дуров уехал из России и перестал управлять «ВКонтакте»). Обсуждалась и публикация BBC о марше за «федерализацию Сибири». Сотрудник Роскомнадзора предлагал их заблокировать и писал: «Люди с острова охамели»; Прокопенко напомнил, что «там [в Британии] *Russia Today* может пострадать». В итоге Роскомнадзор не тронул BBC; проверять российский филиал корпорации ведомство начало в начале 2019 года — фактически в качестве прямого ответа на интерес британских властей к *Russia Today*.

Прокопенко — сын генерала ФСБ и выпускник Военного университета и Академии госслужбы при президенте России. Какое-то время он работал корреспондентом в ИТАР-ТАСС (иногда такие должности служат прикрытием для разведчиков), потом — в Госдуме и прокремлевских молодежных движениях. В администрацию президента его привел Вячеслав Володин, которого после массовых протестов назначили ответственным за российскую внутреннюю политику.

Вся деятельность Прокопенко в начале 2010-х напоминала то, что делал в 1970-х в США Говард Хант — сотрудник администрации президента Никсона, ставший одним из главных фигурантов Уотергейтского скандала. Хант в итоге почти три года отсидел в тюрьме — переписку Прокопенко никто даже не расследовал, хотя из нее следует, что Кремль занимается цензурой и преследованием оппозиции. Прокопенко и сейчас работает в администрации президента.

В интервью (их давали в крипточатах) пресс-секретари «Анонимного интернационала» Шалтай и Болтай утверждали [\[339\]](#), что публикуют сливы, потому что их «не устраивают ограничение свободы в сфере интернета и агрессивная внешняя политика», а также другие особенности российской политики: нечестные выборы и даже плохие условия, созданные для малого и среднего бизнеса. Своей целью «Анонимный интернационал» объявлял [\[340\]](#) «измене-



ние мира к лучшему, хотя бы к большей свободе и информированности общества».

Один из членов группировки цитировал [\[341\]](#) фильм «Хранители»: «Мы делаем это потому, что вынуждены. Когда человек хоть раз видит черную изнанку общества, он больше никогда не обернется к ней спиной».

\*\*\*

В твиттере группировки я нашел их электронную почту и написал письмо с предложением встретиться. «Насколько я понимаю, вы находитесь не в Москве и не в России. Или кто-то есть и здесь?» — спросил я. Они ответили в тот же день: «Немного ошибаетесь) Мы НЕ встречаемся в Москве или в других городах России. Практически все члены команды — граждане РФ и большая часть проживает на территории РФ. Но наши представители и правда встречаются исключительно за пределами РФ. В ближайший месяц наши представители могут встретиться в следующих местах: Стамбул, Бейрут, Бангкок, Киев. Точное время и точное место на территории любого из этих городов — за нами». Я спросил, когда им удобно встретиться в Стамбуле.

Через две недели они написали: «Из Стамбула человек уехал. Возможно, там не появится больше (Есть люди в Бейруте, Киеве, Бангкоке». Еще через неделю выяснилось, что встреча возможна только в Юго-Восточной Азии, лучше всего — в Бангкоке. Я ответил, что это слишком далеко. «Зато тут тепло, недорогое спиртное и женщины))) Шутка))), — ответили они. — Ну тогда как потеплеет) а то поближе холодно)». «Да ладно, мороз бодрит. Может, поближе?» — написал я.

— Ну если серьезно, то есть еще причины [не встречаться ближе].

— Думаете, вышли на ваш след? — спросил я.

— Думаем не вышли))) У нас много следов. Да и не боимся мы ничего если честно)) Хочешь верь, хочешь не верь чисто семейные мотивы))) Все мы люди, все человеки))).

В декабре 2014 года я написал им, что собираюсь в отпуск в Гонконг и смог бы оттуда заехать в Бангкок. Они согласились и посоветовали лететь эфиопскими авиалиниями, потому что «там очень прикольные стюардессы — эфиопки: темная кожа и голубые глаза». Были и другие советы: «В Гонконге в период Сочельника и Рождества (католических) перекрывают центр даже для пешеходов. Поэтому не удивляйся, если вечером 26-го ты увидишь, что в центре пешеходов будут направлять полицейские в обход каких-то улиц. Сам удивился, когда в первый раз увидел, так и не понял почему. И если гостиницу не бронировал, то поторопись. Цены на эти даты в Гонконге традиционно высокие».

\*\*\*



Прилетев в Бангкок, я сразу же купил сим-карту и написал сообщение на нужный номер. Приехав в отель, я стал ждать. Они позвонили через несколько часов и назначили встречу в самом людном районе города — на Каосан-роуд. Алекс Гарленд в романе «Пляж» описывал эти места как «страну пеших туристов»: «Почти все здания на ней превращены в гостиницы... В кафе крутят по видео новейшие американские фильмы; вы не пройдете и нескольких метров, чтобы не наткнуться на ларек, торгующий пиратскими кассетами. Улица служит своего рода кессонной камерой для тех, кто только что приехал в Таиланд или собирается покинуть эту страну, лежащую как раз на полпути между Востоком и Западом».

В январе 2015 года район выглядел примерно так же. Каждый второй европеец прогуливался, держа за руку тайскую проститутку; веселые местные дельцы то и дело шептали на ухо: «Трава? Трава есть. Любовь? Любовь есть». Я немного заплутал, заглядевшись на прилавки, на которых продавали аудиокассеты — в том числе почему-то с российской поп-музыкой конца 1990-х.

Человек из «Шалтая» перезвонил — теперь с другого номера — и попросил подойти к дому № 6 на соседней улице. Когда я подошел к зданию, мужчина на противоположной стороне улицы помахал мне рукой.

Я перебежал дорогу, пока он ловил моторикшу. На встречу пришел улыбчивый мужчина в соломенной шляпе и легкой летней одежде; через плечо у него была перекинута небольшая сумка для ноутбука. Он, конечно, не стал представляться, но я решил называть его Льюисом: участники группировки считали, что «Алиса в стране чудес» с ее вывернутой наизнанку логикой наиболее точно описывает мир российской политики.

Тук-тук сразу же сорвался с места, разогнался и начал петлять между автомобилями. Льюис сразу же начал рассказывать о деятельности группировки, но на улице было так шумно, что я слышал только отдельные слова: «побочный продукт других игр», «представители башен», «Прокопенко», «план работы по себе».

Минут через 15 тук-тук остановился в центре Бангкока. Льюис протянул водителю пару купюр, уточнив, что поездки тут стоят очень мало, и предложил зайти в метро, чтобы точно убедиться, что за нами нет хвоста.

«Мы должны были встретиться недавно с российским журналистом, — объясняет он. — Ну, у нас массивов [информации] много — проверили. Оказалось, что его почту вскрыли [сам] понимаешь кто, и за ним слежка. Пришлось с ним встречу отменить в последний момент. Тебя проверили, за тобой ничего не нашли. Но я все равно попросил Болтая проследить, нет ли за нами хвоста».

— Болтай тоже здесь? — уточнил я.

— Да, он здесь живет. А я приехал на один день передать файлы. Когда у тебя несколько гигабайт информации, иногда проще просто жесткий диск передать лично, чем передавать по сети. Вся информация у нас хранится минимум в двух копиях в разных стра-



нах. И нет человека, который имеет полный доступ ко всему. С Болтаем хотели сегодня искупаться в бассейне в его кондоминиуме, но холодно.

— Пойми, «Анонимный интернационал» — это не моя и не наша основная работа, — продолжил Льюис. — Мы не занимаемся ей постоянно. «Шалтай-Болтай» — это побочный продукт других игр. Мы занимаемся IT-безопасностью и... Как это сказать?

— Опасностью?

— Да. И IT-опасностью.

— Взломами?

— Неточная формулировка. Мы занимаемся получением доступа. Не обязательно путем взлома.

— Но взломать можете?

— Конечно. Но чаще доступ или информацию можно получить другими путями. Например, сходить за человеком в кафе, посмотреть, что он набирает [на клавиатуре]. Иногда, чтобы получить информацию, нужно убеждать. Иногда добрым словом, иногда другим, иногда деньгами, иногда менять одну информацию на другую информацию. Часто проходят мимо нас проекты, тесно связанные с Кремлем. После основной работы всегда остается то, что не пригодились. Эта информация попадает в «Анонимный интернационал».

— У вас много клиентов?

— У нас есть постоянный небольшой круг клиентов. Нам хватает. Ценник на нашу работу начинается от нескольких десятков тысяч долларов. Про верхнюю планку говорить не буду. Нам всем хватает на жизнь и путешествия.

— Кто ваши заказчики? Кому вы продаете информацию?

— По нашей основной работе мы получаем заказы и от государственных структур, и от частных лиц. Никогда не работаем с теми, кто связан с наркотиками. Но мы утверждаем, что мы независимая команда. Просто часто невозможно понять, кто заказчик. Бывает, добываем информацию для посредников, не зная конечного заказчика.

В тот момент никто не знал, кто стоит за «Анонимным интернационалом». Многие гадали: одни думали, что это сам Тимур Прокопенко, другие — что люди еще одного сотрудника администрации президента Алексея Громова (поскольку про него не было публикаций), третьи — что это Владислав Сурков. «Самое смешное, что всем как-то вообще параллельно, ну типа есть и есть, — говорил мне один из сотрудников управления внутренней политики. — Вначале все на шухере были, летом, например, а сейчас нет. Вообще, тут все вроде как бьются очень давно [чтобы найти их]. Одна группа в свое время даже дошла в своих поисках до Лондона, а потом следы теряются. Но большинство мыслей о конторе (то есть о ФСБ. — Прим. Авт.). У чуваков уйма информации, и их никто не может спалить».

— Мы знаем, что нас ищут, — продолжал Льюис. — С мая работает по нам один генерал, сначала работало МВД, потом ФСБ и ФСО. У нас есть десяток эсэмэсок Прокопенко, в которых этот генерал до-



кладывает, что вот-вот, мы уже близко, почти подобралась, ага. Летом через посредников на нас вышли люди, которые попросили взломать аккаунты «Анонимного интернационала», конечно, не зная, что мы — это они и есть. И главной целью ставили не взлом, а последующее выяснение личностей участников. Мы заломили ценник в 100 тысяч долларов. И они отказались. Хотя я не очень понимаю этого, потому что цена-то и не такая большая.

(Уже после нашей встречи, в 2015 году, «Шалтай-Болтай» начал не только выкладывать архивы переписок, но и продавать их на интернет-биржах. На сайте Joker.buzz группировка заключила сделок на 1000 биткоинов — около 275 тысяч долларов по тогдашнему курсу; на февраль 2019 года — 3,4 миллиона долларов.)

— Значит, ваша основная работа — это сбор компромата?

— Нет. Мы занимаемся изменением реальности. Иногда по работе нужно не просто собрать информацию.

— Ничего непонятно.

— У О'Генри есть рассказ — не помню название — про то, как молодой человек никак не может сделать предложение девушке, потому что она очень занята (имеется в виду рассказ «Золото и любовь». — *Прим. Авт.*). И вот случается так, что молодой человек попадает с этой девушкой в пробку, еще какие-то события происходят, и он объясняется ей в любви. А потом к отцу приходит человек со сметой: вот столько нужно заплатить таксистам, вот это полицейским, всем, кто участвовал в пробке. Мы занимаемся примерно тем же. Чтобы человек оказался или не оказался в определенном месте, чтобы информация была выложена в определенный момент.

— Приведите пример изменения реальности.

— По основной работе мы добились отставки губернатора. Положили нужному человеку на стол папочку. Я не буду называть имена.

— Кто принимает решение о публикации файлов?

— Все вместе обсуждаем. Но могу и я один принять решение опубликовать.

— Что вызывало больше всего споров?

— Гиркин, конечно. Болтай у нас самый радикальный, говорил: «Выкладывать по полной нужно этого гондона». Шалтай наоборот. Ну а техникам было по барабану. А Прокопенко не вызывал споров. То, что мы выложили тогда сначала фотографию Потупчик [с деньгами], было открыткой Прокопу. Он сразу понял, что у нас есть. Вообще, мы выкладываем только общественно полезную информацию. Никогда не выкладываем личную.

— Значит, запрет только на личную?

— Мы не будем никогда публиковать гостайны.

— Если бы у вас были данные вроде файлов Сноудена, выложили бы?

— Скорее, нет. Не всё нужно выдавать.

— А если файлы говорят о государственном преступлении?

— Тогда выложим.



— Но Сноуден выложил файлы о государственном преступлении.

— То, что он выложил, всем специалистам знающим было давно известно.

— Как файлы к вам попадают, кроме взлома? Кто источники?

— Некоторым сотрудникам администрации президента нравится, что они причастны к борьбе. Когда приезжаю в Москву, встречаемся с некоторыми за ланчем, я даю информацию, мне дают информацию. В основном источники — это многолетние знакомые там. Но некоторые дают информацию нам по основной работе, не зная, что мы «Анонимный интернационал». А вот с незнакомыми инициативщиками мы не работаем. Очень сложно проверить.

— Про кого будут следующие сливы?

— У нас примерно два терабайта файлов. Есть много файлов о людях, близких к ВВП (то есть к Путину. — *Прим. Авт.*). По Прокопенко мы выложили только 10 %. У нас 40 тысяч SMS, там большая переписка с либеральными журналистами, например. Знаем, что самая частая версия, что работаем на Громова, но то, что ничего не публиковалось о нем, не значит, что ничего не будет опубликовано.

— Значит, будет?

— Я сказал: не значит, что ничего не будет опубликовано.

— Почему такое внимание Прокопенко уделяете?

— Мы за Прокопенко наблюдаем больше двух лет. Сейчас он переходит на другую работу (вместо информационной политики чиновник в декабре 2014 года занялся в структурах администрации президента федеральными выборами — взаимодействием с партиями, Центризбиркомом, молодежными организациями. — *Прим. Авт.*). Нам показалось важным показать напоследок, чем он занимался в последнее время.

Льюис достал из сумки ноутбук, долго рылся в файлах, развернул экран ко мне. На нем был Дмитрий Медведев, развалившийся на стуле в рабочем кабинете, на его столе лежало много разноцветных папок. «Вот на столе папочки, в них самое интересное, до них бы добраться», — сказал Льюис.

По его словам, после публикаций «Анонимного интернационала» в администрации всем сотрудникам запретили пользоваться нерабочей почтой. Теперь у каждого есть защищенный ящик, на который можно зайти только с определенного IP и с определенного компьютера, но, объяснял Льюис, все сотрудники выше помощника вице-премьера эти предписания не соблюдают: «Не придет же фэс-эошник к Дворковичу и не скажет: „Ну-ка, давай-ка выключай“».

Мы вышли из метро на улицу.

— Я когда тебя увидел — с рюкзаком и наушниками, — подумал, что ты легко можешь меня и записать, и сфотографировать, — сказал Льюис. — И выложить завтра мою фотографию.

— И что вы тогда делать будете? Если выложу.

— Больше не приеду в Россию. Напротив твоей фамилии поставлю галочку и при случае подставляю. Ну, а так? Прокопенко киллеров



пришлет, что ли? Хотя... Ну как меня можно найти в Азии? Это невозможно.

Я спросил, можно ли сфотографировать его ноутбук или шляпу [342]. Он запретил фотографировать компьютер, а шляпу повесил на забор — так, чтобы не было никаких вывесок на фоне. «Очень легко потом приехать сюда, дать денег и получить записи с камер наблюдения», — объяснил Льюис, покупая на улице апельсиновый сок. Он достал из сумки небольшую бутылку джина, отхлебнул; достал из кармана одноразовый телефон, который использовал для связи со мной. Платком стер отпечатки пальцев, вынул сим-карту и аккумулятор, выбросил их в разные мусорные ящики и убежал на поезд в аэропорт.

\*\*\*

10 ноября 2017 года в аэропорту Пулково перед вылетом в Минск задержали гражданина России Владимира Аникеева вместе с подругой. Через три дня его выпустили.

Уже после этого выяснилось, что Аникеев был связан с «Шалтай-Болтаем», и именно с ним я встречался в Бангкоке. «Может быть, у вас были случаи, когда человек попал в аварию, у него сотрясение мозга, то есть люди после этого становятся какие-то такие приторможенные, странные, — вспоминал потом другой участник группировки. — Примерно так же изменился [после задержания] Аникеев. У меня было некое недоверие, и я попросил его сходить в «Жан-Жак» на Таганке и сделать селфи на фоне вывески заведения. Он это сделал. После того, как он прислал мне селфи, я сказал, чтобы он прислал мне фотографию чека, он прислал фотографию чека, это был столик номер пять и была фамилия официантки, там было два кофе. Я позвонил в „Жан-Жак“ попросил эту официантку и спросил: «Вот у вас сейчас был заказ на столике номер пять 10 минут назад. Скажите, там был один мужчина или их было двое?»»

Официантка ответила, что Аникеев был один, но его партнер продолжал сомневаться: как можно выпить две чашки кофе за десять минут? По словам участника группировки, Аникеев признал, что спецслужбы обсуждали с ним деятельность «Шалтая-Болтая», но утверждал, что «все вопросы основные решены, а какие-то детали утрясаются». «[Аникеев] говорил, что по договоренности с теми людьми, которые помогли решить этот вопрос, проект дальше может работать, но все участники должны приехать в Россию и находиться под контролем в целях их же безопасности», — рассказывает участник «Шалтая-Болтая». В итоге Аникеев уговорил одного из компаньонов приехать в Россию — после чего сотрудники ФСБ сразу задержали и самого Аникеева, и приехавшего, и еще нескольких участников «Шалтая».

В марте 2017 года в квартиру, в которой я жил до 18 лет и в которой до сих пор живут мои родственники, пришли сотрудники ФСБ. Они искали меня и оставили повестку с вызовом на разговор.



Не зная, чего ожидать, на следующий день я приехал в родной район. Обычно я чувствовал себя там спокойно, но теперь все ощущалось иначе. В знакомом дворе я вглядывался в прохожих, высматривая мужчин в темных костюмах не по размеру, но нашел там только нескольких женщин, привычно беседующих на лавке у подъезда.

Через день я отправился в Лефортово — главное следственное управление ФСБ, которое находится в одном здании с одноименным СИЗО. Расположено это здание за восьмиэтажным жилым домом, к которому прилегает детская площадка; рядом — несколько кафе, в которых родственники обвиняемых обычно встречаются с адвокатами.

Я знал, что на проходной нужно будет сдать телефон, поэтому оставил его в автомобиле: подумал, что оставить его в руках ФСБ — значит фактически согласиться на прослушку и взлом. На проходную пришел следователь, представившийся Ястребовым. Он провел меня наверх. Выйти обратно без него бы не получилось: лабиринт коридоров петлял, лестницы уходили то влево, то вправо, коридоры начинались между этажами и тянулись очень далеко.

Около кабинета следователя из стены торчала металлическая конструкция с прикрепленными наручниками. «Для допросов?» — спросил я. «Ну да», — пошутил Ястребов. В кабинете на потертом линолеуме стоял стол, заваленный бумагами, и большой серый металлический сейф; на двери висел календарь с портретом Феликса Дзержинского.

Ястребов сообщил, что им не разрешают пользоваться интернетом, поэтому он не читал мой репортаж о встрече с «Шалтаем-Болтаем». Чтобы получить доступ к тексту, следователю нужно было записываться в список на листке, ждать очереди, получить ключи, после чего можно было зайти в комнату, где стоял компьютер, подключенный к интернету. Телефоны следователи, как и посетители, сдавали на входе в здание.

Ястребов расспрашивал о встрече с Аникеевым в Бангкоке и попросил пересказать весь репортаж. Через несколько часов следователь предложил выйти покурить. Мы прошли этаж насквозь и остановились около коридора, перекрытого решеткой. «А тут начинается тюрьма, сюда лучше никогда не попадать», — сказал следователь. «Ага», — кивнул я, докуривая.

\*\*\*

Аникеева обвинили в нескольких взломах. Его дело рассматривалось публично, хотя обычно такие заседания проходят в закрытом режиме.

Пока Аникеева судили, участник группировки, оставшийся на свободе, — он называл себя Шалтай, — обратился в СМИ с предложениями дать интервью. Он встретился в Риге с «Медузой», потом [\[343\]](#) — с «Дождем» в Таллине, где решил просить политическое убе-



жище. С журналистами он разговаривал, видимо, в надежде ускорить этот процесс.

Звали Шалтая Александр Глазастиков. Он сообщил, что, раз других участников группировки поймали, скрывать ему нечего — наверняка спецслужбы всё о нем знают. Глазастиков рассказал, что будущие участники «Анонимного Интернационала» познакомились друг с другом в 2004 году на эротических вечеринках Дмитрия Грызлова — сына политика Бориса Грызлова, долгое время руководившего «Единой Россией» и Госдумой. Потом они периодически общались, но «Шалтай-Болтай» придумали только в 2013 году. Аникеев к тому моменту около десяти лет занимался «черным пиаром» и обзавелся кругом знакомых в правительстве и около него, которые сливали ему инсайдерскую информацию.

Одни из первых документов «Шалтай-Болтай» получил после того, как их знакомые хакеры провели массовую фишинговую рассылку по российским чиновникам. После этого «Шалтай» получил контроль над несколькими ящиками; некоторые чиновники так и не узнали, что их взломали.

«Организация создавалась с политической целью, чтобы раскрыть тайны о лицах, связанных с правительством России, с президентской администрацией», — объяснял Глазастиков. Раскрывать тайны он хотел выборочно: например, не трогать спецслужбы. Коллеги думали иначе. В августе 2015 года группировка опубликовала открытое письмо контрразведке. В нем говорилось, что им удалось вскрыть почтовые ящики высокопоставленных сотрудников Минобороны. «Мы с сожалением убедились в полной некомпетентности сотрудников ряда подразделений Министерства обороны РФ в области информационной безопасности, а если говорить более конкретно — в преступной небрежности, — заявил «Шалтай-Болтай». — Через бесплатные почтовые сервисы типа Yandex.ru, Mail.ru и американский mail.com передавались незашифрованные служебные документы, часто представляющие собой секретную информацию, связанную с обороноспособностью РФ». В почтовых переписках чиновников оказались пароли для служебных серверов других подразделений Минобороны.

Глазастиков уверен, что именно после этого за ними активно начали охотиться. Вскоре знакомые сообщили хакерам, что в ГРУ знают их настоящие имена. Видимо, после этого ФСБ вышла на контакт с Аникеевым и встретила с ним в Москве. Группировке пообещали спокойное будущее при условии, что однажды они смогут через «Шалтая» опубликовать какую-то свою информацию. Глазастиков думает, что с Аникеевым общался Сергей Михайлов, работавший тогда в ЦИБ ФСБ и курировавший хакеров. Михайлова задержали вскоре после ареста Аникеева, но адвокат «Льюиса» утверждал, что обвинения в адрес сотрудника ФСБ никак не связаны с «Шалтаем-Болтаем».

Аникеева в итоге приговорили к двум годам тюрьмы; других участников «Шалтая» — к трем; Глазастиков получил убежище и



остался в Эстонии. Архивы, выложенные группировкой, и сейчас остаются одним из главных источников информации о том, как на самом деле устроена внутренняя политика в России.

В августе 2018 года Аникеев вышел из тюрьмы. Хакер снова оказался на свободе — и заявил, что теперь займется обеспечением кибербезопасности. Работа для него в ближайшие годы точно найдется.



## Благодарности

«Краткая история русских хакеров» никогда бы не получилась без поддержки моих друзей.

Эльнаре Ялалтдиновой — <3; Юрия Болотова и Кирилла Демченко, которые спрашивали, когда же я наконец допишу книжку.

Ивана Колпакова, одного из основателей и главного редактора «Медузы», с которым мы решили сделать некоторые истории из этой книги и который разрешил уехать в долгий отпуск.

Редактора отдела специальных корреспондентов «Медузы» Александра Горбачева в 2016-2019 годах, моего главного собеседника о текстах и человека, с которым мы ежедневно их обсуждаем; он же гениально отредактировал эту книгу.

Спасибо «Прогрессу» и «Старлайту» за кофе и вайфай.

Кроме того — я бы не смог написать «Краткую историю русских хакеров» без поддержки *Kennan Institute* в Вашингтоне, которые дали время для поисков.



# Глоссарий

**APT** — целенаправленная хакерская атака.

**DDoS-атака** — способ вывести из строя сайт или сервер, перегрузив их. Как правило, во время атаки очень много устройств, зараженных вирусом, одновременно начинают заходить на один и тот же сайт; он не успевает обработать нагрузку и перестает открываться или работает очень медленно.

**Хостинг** — место хранения данных для сайта в интернете.

**Бот** — программа, которая по расписанию выполняет определенные задачи. В последние годы так называют и живых людей — например, сотрудников «фабрики троллей».

**Трафикообменник** — точка обмена трафиком между провайдерами; их создают и для оптимизации скорости соединений.

**VPN** — самый простой способ скрыть свое реальное местонахождение и адрес в интернете. Виртуальная частная сеть, которая по зашифрованному каналу может соединять компьютеры в разных городах и странах, делая вид, будто они находятся в одной локальной сети.

**Tor** — браузер, который скрывает данные пользователя и позволяет заходить на сайты, не индексирующиеся обычными поисковиками.

**IP-адрес** — уникальный адрес компьютера, подсоединенного к интернету.

**FTP** — протокол передачи файлов между компьютерами.

**IRC** — протокол обмена сообщениями.

**Нейронная сеть** — систему соединенных между собой простых процессоров, которую можно обучить решать задачи. В нейронных сетях может быть несколько уровней, каждый уровень комбинирует признаки предыдущих уровней — то есть создаются все более сложные комбинации, о которых могут даже не знать сами ее создатели.

**Уязвимость нулевого дня** — «дыра» в программном обеспечении, неизвестная производителю.

**Брандмауэр** — инструмент защиты компьютера от хакерских атак, при которой система проверяет все обращения из интернета. То же, что и файрвол.

**Эксплойт** — программа, использующая уязвимость в безопасности другой программы.

**Дамп** — база украденных копий дебетовых и кредитных карт.

**Троян** — вирус, выдающий себя за обычную программу или документ.

**Фишинг** — способ хакерской атаки. Как правило, для фишинга используются поддельные письма от провайдеров, банков, социальных сетей или знакомых, ведущие на зараженные сайты, которые похищают персональные данные жертвы.

**PGP** — технология шифрования писем, позволяющая вести переписку безопасно. При переписке исходящие письма шифруются



специальным ключом; собеседник может расшифровать входящее письмо с помощью другого ключа.

**ГРУ** — Главное разведывательное управление, подчиняющееся Министерству обороны. ГРУ (формально последние годы ведомство называется Главное управление Генштаба, но все всё равно используют прежнюю аббревиатуру) занимается военной и политической разведкой, работает с источниками, проводит секретные операции.

**Управление «К»** — отделение МВД, занимающееся расследованием киберпреступлений.



## Примечания

Примечания и ссылки, собраны на странице <https://individuumbooks.com/vtorzhenie/notes/>

[1] ...сайт компании скромно сообщает, что организация специализируется на «разработке передовых сетевых технологий»: <https://packetstechnologies.bg/bg/> (сейчас сайт недоступен)

[2] ...мощность крупнейшей DDoS-атаки в истории интернета: «DDoS-атака 300 Гбит/с замедлила весь интернет», доступно на <https://xakep.ru/2013/03/27/60346/>

[3] ...ссылку на расследование Reuters: «СМИ узнали об угрозах Касперского „мочить“ конкурентов», доступно на <http://top.rbc.ru/business/29/08/2015/55e0ed279a794742b6f4add8>

[4] ...молодой житель Санкт-Петербурга Кирилл впервые попал на рынок «Юнона»: «Сценерский лайфстайл: часть 1», доступно на <http://xakep-archive.ru/xa/090/088/1.htm>

[5] ...Программист Антон Мельников подробно вспоминал, на какие ухищрения ему и его другу Мише приходилось идти: <https://twitter.com/proxiper/status/1045631964244578304>

[6] ...Участники группировки STEALTH рассказывали, что еще в 1994 году внедрились в американское посольство: «Я — создатель боевых машин-убийц!», доступно на <http://xakep-archive.ru/xa/003/036/1.asp.htm>

[7] ...Их коллеги вспоминали, как взламывали сайт Новороссийска: «Российские хак-группы: кто они?», доступно на <http://xakep-archive.ru/xa/026/044/3.asp.htm>

[8] ...в российском издании «Хакер» был опубликован фрагмент манифеста хакеров: «Манифест хакера», доступно на <http://xakep-archive.ru/spec/007/053/1.html>

[9] ...Гофман считался одним из самых перспективных и талантливых российских академических музыкантов: «Альт F4 Ильи Гофмана», доступно на <https://www.kommersant.ru/doc/217749>

[10] ...их называли «змеями из интернета»: «Змеи из интернета», доступно на <http://www.mk.ru/old/article/1999/11/14/133894-zmei-iz-interneta.html>

[11] ...всерьез напугал тогдашнего президента США: Dark Territory: The Secret History of Cyber War, Fred Kaplan (Simon & Schuster, 2017)

[12] ...большой опрос среди посетителей русскоязычных хакерских форумов: «Исследование компьютерного андеграунда на постсоветском пространстве», доступно на <https://bugtraq.ru/library/underground/research.html>

[13] ...распространяться пьеса «История, которой не было, или „Хакнутые выборы-99»: <http://www.rusdoc.ru/material/vzlom/vybory.shtml>

[14] ...вспоминал один из хакеров, начинавший в те годы: «Хакерская группа KZR — изнутри», доступно на <http://xakep-archive.ru/xa/004/032/1.asp.htm>

[15] ...вспоминал участник группировки: там же



[16] ...Как утверждали участники группы в одном из номеров «Хакера»: «Хакерская группа KZR — изнутри», доступно на <http://xakep-archive.ru/xa/004/032/2.asp.htm>

[17] ...они сумели взломать 21 американский сайт: там же

[18] ...писал он в материале, опубликованном в «Хакере» в 1999 году: «Хакерская группа KZR — изнутри», доступно на <http://xakep-archive.ru/xa/004/032/3.asp.htm>

[19] ...Дмитрий стал завсегдаем «Античата»: <http://forum.antichat.ru/>

[20] ...посетители «Античата» фактически жили на сайте — и даже посвящали ему песни: Antichat.ru — NoFear, доступно на [https://www.youtube.com/watch?v=ZRGv6Q3txA&list=PLT5tHbJPR2\\_opfQPmuy6pKd1C\\_qiWV0eD](https://www.youtube.com/watch?v=ZRGv6Q3txA&list=PLT5tHbJPR2_opfQPmuy6pKd1C_qiWV0eD)

[21] ...Объявления выглядят примерно так: <https://blackbiz.club/threads/vzlom-whatsapp-viber-instagram-facebook-uznaem-vzlomaem.5098/>

[22] ...называют создателями WMD: Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Cathy O'Neil (Broadway Books, 2016)

[23] ...После той беседы программирование внесли в перечень дисциплин: «Андрей Станкевич стал медиаперсоной года по версии „Комсомольской правды в Санкт-Петербурге“», доступно на [http://news.ifmo.ru/ru/university\\_live/achievements/news/6802/](http://news.ifmo.ru/ru/university_live/achievements/news/6802/)

[24] ...они рассказывают о подготовке «будущих защитников информационного пространства»: [https://vk.com/video-129090933\\_456239022?api\\_access\\_key=585f3ac8e3e68c4647](https://vk.com/video-129090933_456239022?api_access_key=585f3ac8e3e68c4647)

[25] ...заявлял на конференции о киберпреступности, что «российские хакеры — лучшие в мире»: «Российские хакеры — „лучшие в мире“», доступно на <https://www.securitylab.ru/news/215244.php>

[26] ...писал Перлин: <https://www.facebook.com/maxim.perlin/posts/745204182281015>

[27] ...рассказывал в те годы Андрей Споров, он же хакер Sp0Raw: «Лицом к лицу с хакером», доступно на <https://www.vedomosti.ru/newspaper/articles/2004/11/02/licom-k-licu-s-hakerom>

[28] ...Один из руководителей форума описывал эту иерархию так: «Планета CC. Золотое время Carderplanet», доступно на <https://bugtraq.ru/library/underground/planetacc.html>

[29] ...рассказывал участник Carderplanet: там же

[30] ...Большинство постоянных жителей «Планеты» зарабатывали около 5000 долларов в месяц: «Планета хакеров: как создавался крупнейший в мире форум киберпреступников», доступно на <http://www.forbes.ru/tekhnologii/tekhnika-i-biznes/332679-planeta-khakerov-kak-sozdavalsya-krupneishii-v-mire-forum-kiber>

[31] ...Script объяснял, что занимается кардингом в том числе для развлечения: «Кардинг. Интервью со Script'ом», доступно на <http://xakep-archive.ru/xa/039/048/3.html>



[32] ...рассказывал позже один из кардеров: «„Если бы не стукач, нас бы не нашли“. История белорусского киберпреступника, живущего в США», доступно на <http://belgid.by/news/it/31784>

[33] ...его освободили из-под ареста еще до суда: «Банковские карты легли удачно», доступно на <https://www.kommersant.ru/doc/639299>

[34] ...его освободили из-под ареста еще до суда: «Банковские карты легли удачно», доступно на <https://www.kommersant.ru/doc/639299>

[35] ...Russian Business Network, расцвет которой пришелся на 2006–2007 годы: Shadowy Russian Firm Seen as Conduit for Cybercrime, доступно на [http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461\\_pf.html?noredirect=on](http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html?noredirect=on)

[36] ...Все это нашли и изъяли при аресте у уроженца Крыма Романа Веги: «Система координат», доступно на <https://www.romanvega.ru/p/intro.html>

[37] ...По словам другого бывшего участника «Планеты»: «Эксклюзивное интервью бывшего хакера, отсидевшего за киберворовство в США», доступно на <https://www.youtube.com/watch?v=3VlbPSPN8jE>

[38] ...писал Вега в своем блоге: «Система координат», доступно на <https://www.romanvega.ru/p/intro.html>

[39] ...Бывший хакер Дмитрий Насковец рассказывал: «Как кардер вышел из тюрьмы и делает бизнес на кибербезопасности», доступно на <https://secretmag.ru/trends/players/naskovets-hacker.htm>

[40] ...хакер ответил гневным письмом: <https://docs.google.com/file/d/0ByQf4BUGl49wSVV0Uk45U3doS1U/edit>

[41] ...Павлович признавался, что «никогда не смог бы украсть кошелек в общественном транспорте»: <https://tgraph.io/Intervyu-s-izvestnym-karderom-08-10>

[42] ...Павловича считали участником группировки, совершившей «крупнейшее хищение в истории США»: Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U. S. Retailers, доступно на <https://www.justice.gov/archive/opa/pr/2008/August/08-ag-689.html>

[43] ...Среди прочего Павлович опубликовал материал о своих бизнес-планах: <https://carding.pro/ru/vodke-carder-i-hacker-byt/>

[44] ...Владислав Хорохорин сидел с коктейлем в зале ожидания: «Планета хакеров: как создавался крупнейший в мире форум киберпреступников», доступно на <https://www.forbes.ru/tekhnologii/tekhnika-i-biznes/332679-planeta-khakerov-kak-sozdavalsya-krupneishii-v-mire-forum-kiber>

[45] ...рассказывал его соратник по Carderplanet: «Как я украл миллион. Исповедь раскаявшегося кардера», Сергей Павлович (Питер, 2014)

[46] ...В 2007 году Хорохорин выпустил мультфильм в двух частях: А BadB Welcome Cartoon, доступно



на [https://www.youtube.com/watch?v=O\\_hP-Mrhv7U](https://www.youtube.com/watch?v=O_hP-Mrhv7U),  
<https://www.youtube.com/watch?v=CEAMeVYqzSw>

[47] ...хакер рассказал, что, находясь в заключении, он нашел «дыры» в безопасности американских военных организаций: «Эксклюзивное интервью бывшего хакера, отсидевшего за киберворовство в США», доступно на <https://www.youtube.com/watch?v=3VlbPSPN8jE>

[48] ...Вот что он рассказал: [https://www.nytimes.com/interactive/2017/04/21/technology/document-Seleznev-Letter.html?\\_r=0](https://www.nytimes.com/interactive/2017/04/21/technology/document-Seleznev-Letter.html?_r=0)

[49] ...Все кафе взорвалось: «Раненного в Марокко сына депутата везут в Москву для срочной операции», <https://ria.ru/20110429/369552620.html>

[50] ...Как указано в материалах уголовного дела Селезнева: <https://krebsonsecurity.com/wp-content/uploads/2014/07/Seleznev-Indictment-CR11-0070RAJ-1.pdf>

[51] ...Известно, что только через один из сервисов для переводов он получил около 18 миллионов долларов: там же

[52] ...как у другого арестованного российского хакера Евгения Никулина: <https://www.justice.gov/opa/press-release/file/904516/download>

[53] ...Отец Селезнева предложил ввести против Мальдив экономические санкции: «Хакер Роман Селезнев: взгляд из Москвы», доступно на <https://www.golos-ameriki.ru/a/vv-seleznev/1953487.html>

[54] ...Он рассказывал, что Романа возят на восьми бронированных автомобилях: «„Украинский след“ в деле Селезнева», доступно на <https://www.gazeta.ru/social/2014/08/09/6168613.shtml>

[55] ...Прокурор заявил, что Селезнев — самый серьезный киберпреступник: Russian hacker called „Tony Soprano-style mob boss“ is sentenced in Seattle to 27 years, доступно на <https://www.seattletimes.com/seattle-news/crime/prolific-russian-hacker-who-raked-in-millions-sentenced-to-27-years-in-prison/>

[56] ...Его приговорили к 27 годам: Russian Cyber-Criminal Sentenced to 27 Years in Prison for Hacking and Credit Card Fraud Scheme, доступно на <https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-27-years-prison-hacking-and-credit-card-fraud-scheme>

[57] ...В сентябре 2017 года Селезнев признал обвинения еще по двум делам: Russian Cyber-Criminal Pleads Guilty To Role In Organized Cybercrime Ring Responsible For \$50 Million In Online Identity Theft, доступно на <https://www.justice.gov/usao-nv/pr/russian-cyber-criminal-pleads-guilty-role-organized-cybercrime-ring-responsible-50>

[58] ...Он стал соучредителем компании YouDo и написал о запуске сайта колонку для roem.ru: «YouDo: с Porucheno.ru мы не конкуренты», доступно на <https://roem.ru/25-03-2009/128464/youdo-s-poruchenu-my-ne-konkurenty/>

[59] ...говорил певец в 2010 году: «Одна звезда Владимира Кузьмина», доступно на



[https://www.mk.ru/culture/interview/2010/05/30/500105-odna-zvezda-  
vladimira-kuzmina-foto.html](https://www.mk.ru/culture/interview/2010/05/30/500105-odna-zvezda-vladimira-kuzmina-foto.html)

[60] ...В 2016 году певец уже отрицал родство с хакером: «Владимир Кузьмин не признает родство с известным хакером», доступно на [https://www.vesti.ru/videos/show/vid/681412/cid/1741/#/video/https%3A%2F%2Fplayer.vgtrk.com%2Fframe%2Fvideo%2Fid%2F1530869%2Fstart\\_zoom%2Ftrue%2FshowZoomBtn%2Ffalse%2Fsid%2Fvesti%2FisPlay%2Ftrue%2F%3Facc\\_video\\_id%3D681412](https://www.vesti.ru/videos/show/vid/681412/cid/1741/#/video/https%3A%2F%2Fplayer.vgtrk.com%2Fframe%2Fvideo%2Fid%2F1530869%2Fstart_zoom%2Ftrue%2FshowZoomBtn%2Ffalse%2Fsid%2Fvesti%2FisPlay%2Ftrue%2F%3Facc_video_id%3D681412)

[61] ...рассказывала мать хакера Татьяна Артемьева: «Первая жена Владимира Кузьмина: В смерти моих детей виновата Алла Пугачева!», доступно на [https://sobesednik.ru/shou-biznes/pervaya-zhena-  
vladimira-kuzmina-v-smerti-moikh-detei-vinovata-alla-pugacheva](https://sobesednik.ru/shou-biznes/pervaya-zhena-vladimira-kuzmina-v-smerti-moikh-detei-vinovata-alla-pugacheva)

[62] ...В материалах уголовного дела Кузьмина указано: Nikita Kuzmin, Creator Of The Gozi Virus, Sentenced In Manhattan Federal Court, доступно на [https://www.justice.gov/usao-sdny/pr/nikita-kuzmin-  
creator-gozi-virus-sentenced-manhattan-federal-court](https://www.justice.gov/usao-sdny/pr/nikita-kuzmin-creator-gozi-virus-sentenced-manhattan-federal-court)

[63] ...Он указывал, что, сдавая вирус в прокат: US Sentences Proponent of «Hacker-for-Hire» Cybercrime, доступно на [https://www.voanews.com/a/us-sentences-proponent-of-hacker-for-  
hire-cybercrime/3312942.html](https://www.voanews.com/a/us-sentences-proponent-of-hacker-for-hire-cybercrime/3312942.html)

[64] ...Кузьмина защищал Алан Футерфас: All the president's men's lawyers: who are Trumpworld's leading attorneys?, доступно на [https://www.theguardian.com/us-news/2017/jul/15/donald-trump-  
russia-lawyers-kasowitz-futerfas](https://www.theguardian.com/us-news/2017/jul/15/donald-trump-russia-lawyers-kasowitz-futerfas)

[65] ...та якобы предлагала сотрудникам президентского штаба Трампа компромат: «Сын Трампа встречался с „адвокатом из Кремля“ ради компромата на Хиллари Клинтон. При посредничестве певца Эмина Агаларова», доступно на [https://meduza.io/feature/2017/07/11/syn-donalda-trampa-  
vstrechalsya-s-advokatom-kremlya-radi-kompromata-na-hillari-klinton-pri-  
posrednichestve-pevtsa-emina-agalarova](https://meduza.io/feature/2017/07/11/syn-donalda-trampa-vstrechalsya-s-advokatom-kremlya-radi-kompromata-na-hillari-klinton-pri-posrednichestve-pevtsa-emina-agalarova)

[66] ...он участвовал в обсуждении инициативы администрации президента: [https://roem.ru/29-02-2016/220224/bank-fns-  
tranborder/#comment-219896](https://roem.ru/29-02-2016/220224/bank-fns-tranborder/#comment-219896)

[67] ...Приговор хакеру огласили 2 мая 2016 года: Nikita Kuzmin, Creator Of The Gozi Virus, Sentenced In Manhattan Federal Court, доступно на [https://www.justice.gov/usao-sdny/pr/nikita-kuzmin-creator-gozi-  
virus-sentenced-manhattan-federal-court](https://www.justice.gov/usao-sdny/pr/nikita-kuzmin-creator-gozi-virus-sentenced-manhattan-federal-court)

[68] ...Судя по фейсбуку Кузьмина, теперь он занимается площадкой для трейдинга: <https://www.facebook.com/nikita.kouzmin>

[69] ...Дмитрий «Смелый» Смилянец объявил, что у команды появляется «куратор»: [http://forum.navi.gg/counter-  
strike\\_obschiy/v\\_moscow\\_five\\_poyavilsya\\_kurator\\_proekta/](http://forum.navi.gg/counter-strike_obschiy/v_moscow_five_poyavilsya_kurator_proekta/)

[70] ...бизнесмен и долларовый миллиардер Сергей Матвиенко: «„Империя“ Матвиенко: чем владеет сын губернатора Петербурга», доступно на [https://www.dp.ru/a/2009/12/08/Imperiya\\_Matvienko\\_chem](https://www.dp.ru/a/2009/12/08/Imperiya_Matvienko_chem)

[71] ...он выложил фотографию избирательного бюллетеня: [https://vk.com/wall130960779\\_290](https://vk.com/wall130960779_290)



[72] ...он выложил фото с круглого стола: [https://vk.com/wall130960779\\_279](https://vk.com/wall130960779_279)

[73] ...он выкладывал картину «Благословенное утро в Москве»: [https://vk.com/ddd1ms?w=wall130960779\\_368](https://vk.com/ddd1ms?w=wall130960779_368)

[74] ...по данным Bloomberg, Смилянец познакомился с Владимиром Дринкманом: Biggest U. S. Hack Case Is Tale of Gamers' Interrupted Vacation, доступно на <https://www.bloomberg.com/news/articles/2015-01-12/biggest-u-s-hack-case-is-tale-of-gamers-interrupted-vacation>

[75] ...По данным американского уголовного дела: Russian National Admits Role in Largest Known Data Breach Conspiracy Ever Prosecuted, доступно на <https://www.justice.gov/opa/pr/russian-national-admits-role-largest-known-data-breach-conspiracy-ever-prosecuted>

[76] ...на sports.ru вышла колонка: <https://cyber.sports.ru/tribuna/blogs/explosivesheep/834007.html>

[77] ...считает, что вина его сына не подтверждается никакими доказательствами: [https://vk.com/vipsmi?w=wall222255116\\_14](https://vk.com/vipsmi?w=wall222255116_14)

[78] ...Он заявил Bloomberg, что прочитал в голландской тюрьме «Песнь льда и пламени»: Biggest U. S. Hack Case Is Tale of Gamers' Interrupted Vacation, доступно на <https://www.bloomberg.com/news/articles/2015-01-12/biggest-u-s-hack-case-is-tale-of-gamers-interrupted-vacation>

[79] ...как он вспоминал позже: «Белорусский „хакер“, осуждённый в США: „Меня арестовывали 40 человек — Интерпол, ФБР, полиция”», доступно на <https://dev.by/news/beloruskiy-haker-osuzhdyonnyy-v-ssha-menya-arestovyvali-40-chelovek-interpol-fbr-cheshskaya-politsiya>

[80] ...Сбербанк в июне 2016-го оценил потери экономики России от киберпреступности: «Сбербанк оценил потери экономики РФ от кибератак за год в 600 млрд. рублей», доступно на <http://www.interfax.ru/business/512912>

[81] ...В первом докладе о результатах работы Fincert: [https://www.cbr.ru/StaticHtml/File/14435/FinCERT\\_survey.pdf](https://www.cbr.ru/StaticHtml/File/14435/FinCERT_survey.pdf)

[82] ...Позже оказалось, что Lurk устроен как модульная система: «Охота на Lurk», доступно на <https://securelist.ru/the-hunt-for-lurk/2922>

[83] ...Задержание хакеров из Lurk выглядело как боевик: «Задержание хакеров», доступно на [https://www.youtube.com/watch?time\\_continue=286&v=JOTldBlmntw](https://www.youtube.com/watch?time_continue=286&v=JOTldBlmntw)

[84] ...Изъяли украшения на 12 миллионов рублей и оружие: «Штаб-квартира хакеров, похитивших более 1,7 миллиардов рублей у банков, была в Екатеринбурге», доступно на <https://www.ural.kp.ru/daily/26537.4/3553523/>

[85] ...заявлял, что никто из подозреваемых не пойдет на сделку со следствием: «Троянцу подобрали команду», доступно на <https://www.kommersant.ru/doc/3292947>

[86] ...объяснял он: там же



[87] ...объяснял Алексей Лукацкий, работающий консультантом по информационной безопасности в Cisco Systems: «Антон Носик: Откуда в России хакеры?», доступно на <https://snob.ru/selected/entry/13263>

[88] ...можно найти ролики о последнем уровне «глубокого интернета»: «Проверка интернет легенд — Тихий дом», доступно на [https://www.youtube.com/watch?v=TFtuOdvY\\_is](https://www.youtube.com/watch?v=TFtuOdvY_is)

[89] ...где якобы хранится информация «о боге/смерти/жизни и все, что только захотите»: [https://netstalking.fandom.com/ru/wiki/Тихий\\_дом](https://netstalking.fandom.com/ru/wiki/Тихий_дом)

[90] ...арестовали и назвали «крупнейшим посредником для распространения детской порнографии на планете»: «Основатель Freedom Hosting арестован в Ирландии и ждет экстрадиции в США», доступно на <https://habrahabr.ru/post/188914/>

[91] ...ФБР после заявляло, что контролировало серверы еще до ареста владельца: FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, доступно на <https://www.wired.com/2013/09/freedom-hosting-fbi/>

[92] ...ФБР после заявляло, что контролировало серверы еще до ареста владельца: FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, доступно на <https://www.wired.com/2013/09/freedom-hosting-fbi/>

[93] ...Об этом же писали журналисты Андрей Солдатов и Ирина Бороган: «Кремль и хакеры», доступно на <https://agentura.livejournal.com/51685.html>

[94] ...он рассылал письма: Is Waledac Spam Dirtying the Russian 2012 Elections?, доступно на <https://www.symantec.com/connect/ru/blogs/waledac-spam-dirtying-russian-2012-elections?page=1>

[95] ...Сам Severa рассказывал, что занимается спамом с 1999 года: <https://forum.antichat.ru/threads/vebmajl-rassyiki-ot-severa.294101/>

[96] ...и называл себя «одним из самых живучих спам-королей интернета»: <https://forum.antichat.ru/members/162854/>

[97] ...Жена Левашова рассказывала, что во время обыска: Arrested Russian's wife denies U.S. charge he is global hacking mastermind, доступно на <https://uk.reuters.com/article/us-usa-cyber-botnet-wife/arrested-russians-wife-denies-u-s-charge-he-is-global-hacking-mastermind-idUKKBN1AA17U>

[98] ...обвиняя американские власти: «„Хватают исподтишка": в МИД прокомментировали задержание российского программиста в Испании», доступно на <https://www.ntv.ru/video/1381208/>

[99] ...в 2014 году он взломал компьютеры одной санкт-петербургской больницы: «Программист Левашов заочно арестован», доступно на <https://iz.ru/661226/2017-10-20/programmist-levashov-zaochno-arestovan-v-rossii>

[100] ...в Германии нашли сожженное тело неизвестного мужчины: <http://phrack.org/issues/27/12.html>



[101] ...его участники собирались менять общество с помощью новых цифровых технологий: The Impact of Federal German Intelligence Service Bundesnachrichtendienst (BND) Project RAHAB and Chaos Computing Congresses (CCC) impact on the Future of Computer-Network Mediated Espionage: Cuckoo's Egg Prequel or Perfect Storm?, доступно на <https://www.afcea.org/committees/cyber/documents/impactofbndprojectrahabandcccconthefutureofcomputer-networkmediatedespionage-cuckooseggpreque.pdf>

[102] ...советские чиновники платили и за них: W. German «Hackers» Tricked KGB, Paper Says, доступно на [http://articles.latimes.com/1989-03-06/news/mn-130\\_1\\_west-german](http://articles.latimes.com/1989-03-06/news/mn-130_1_west-german)

[103] ...немецкий телеканал ARD оценил действия хакеров как самый серьезный случай шпионажа: [https://www.washingtonpost.com/archive/politics/1989/03/03/german-computer-hackers-held-for-spying-for-soviets/b2fccb53-4939-48d8-b74e-30d3dcda88cb/?utm\\_term=.c9b3e718065f](https://www.washingtonpost.com/archive/politics/1989/03/03/german-computer-hackers-held-for-spying-for-soviets/b2fccb53-4939-48d8-b74e-30d3dcda88cb/?utm_term=.c9b3e718065f)

[104] ...одних удивляло, что трава вокруг тела сгорела: <http://phrack.org/issues/25/10.html>

[105] ...других — то, что хакер вообще поехал с канистрой бензина: Hans Heinrich Hübner; Ex Member of Chaos Computer Club (CCC), доступно на [http://paolodelbene.pbworks.com/w/page/50465475/Hans%20Heinrich%20Hübner%3B%20Ex%20Member%20of%20Chaos%20Computer%20Club%20\(CCC\)](http://paolodelbene.pbworks.com/w/page/50465475/Hans%20Heinrich%20Hübner%3B%20Ex%20Member%20of%20Chaos%20Computer%20Club%20(CCC))

[106] ...на форумах его иногда называют «великим воином»: <https://www.godlikeproductions.com/forum1/message993360/pg1?disclaimer=1>

[107] ...президент отвечал на них почти теми же словами: <http://kremlin.ru/events/president/news/52830>

[108] ...Несколько студентов Томского политехнического университета организовали «Сибирскую сетевую бригаду»: [https://primerussia.ru/article\\_materials/327.html](https://primerussia.ru/article_materials/327.html)

[109] ...они разместили рисунок: «С Лермонтовым наперевес», доступно на <https://www.kommersant.ru/doc/15879>

[110] ...лидер организации отправил в американские СМИ и Госдепартамент США очередное обращение: «Томские хакеры 3 года ведут информационную войну против чеченских экстремистов», доступно на <https://www.newsru.com/russia/30Jan2002/hakery.html>

[111] ...после этого сайту приходилось переезжать: «Как Россия боролась с „Кавказ-центром"», доступно на [https://www.gazeta.ru/2006/03/09/oa\\_191473.shtml](https://www.gazeta.ru/2006/03/09/oa_191473.shtml)

[112] ...русскоязычные хакеры начали массово распространять вирус: «Не играйте за рулем», доступно на <http://www.itogi.ru/archive/2002/19/97277.html>

[113] ...Мовлади Удугов был уверен, что за действиями хакеров стоит ФСБ: «Пропагандистские ресурсы чеченских сепаратистов



подверглись анонимной экзекуции», доступно на <http://www.membrana.ru/particle/13580>

[114] ...В томском ФСБ публично говорили: «ФСБ не видит нарушения закона в действиях томских хакеров против сайта „Кавказ-центр“», доступно

на <https://www.newsru.com/russia/04feb2002/tomsk.html>

[115] ...создали некоторые хакеры-патриоты: <https://web.archive.org/web/20060323114250/http://www.cyberantiterror.com:80/targets/>

[116] ... Через месяц появился другой похожий проект: «Политподключенные», доступно на <https://www.kommersant.ru/doc/620317>

[117] ...Создатели проекта указывали, что ищут DDoS-специалистов: <https://web.archive.org/web/20051025000535/http://www.peace4peace.com:80/>

[118] ...После нападения боевиков на Нальчик в октябре 2005-го: «В Нальчик пришла война», доступно на <https://lenta.ru/articles/2005/10/13/nalchik/>

[119] ...Один из атакованных банков потратил на восстановление от атаки: «Wikileaks: Эстония отделалась легко», доступно на <https://inosmi.ru/baltic/20101211/164825182.html>

[120] ...атаки называли «первой мировой кибервойной»: Denial-of-Service: The Estonian Cyberwar and Its Implications for U. S. National Security, доступно на <http://www.iar-gwu.org/node/65>

[121] ...Ответственность за организацию атак взял: «Акция хакерского неповиновения», доступно на <https://www.kommersant.ru/doc/1136738>

[122] ...говорил он: Kremlin Kids: We Launched the Estonian Cyber War, доступно на <https://www.wired.com/2009/03/pro-kremlin-gro/>

[123] ...Спецслужбы США считают, что бот-сетью атаки управлял: <https://www.justice.gov/opa/press-release/file/956511/download>

[124] ...Как рассказывал журналист Андрей Солдатов, мужчина представлялся сотрудником: «Кибер-сюрприз», доступно на <https://www.novayagazeta.ru/articles/2007/05/31/33284-kiber-syurpriz>

[125] ...он, например, подробно рассказывал, как взломать онлайн-банк: «Красиво жить не запретишь», доступно на <http://xakep-archive.ru/xa/093/086/1.htm>

[126] ...Там были размещены рекомендации: Inside Cyber Warfare: Mapping the Cyber Underworld, Jeffrey Carr (O'Reilly Media, 2011)

[127] ...заявляли они в своем обращении: <https://web.archive.org/web/20080812013618/http://www.stopgeorgia.ru/>

[128] ...На Stopgeorgia появился список «первоочередных целей»: <https://web.archive.org/web/20080812084132/http://www.stopgeorgia.ru/?pg=tar>

[129] ...Случались в те дни и кибератаки на российские ресурсы: «Сайты заняли оборону», доступно на <https://www.kommersant.ru/doc/1010863>



[130] ...Позже исследователи выяснили: Inside Cyber Warfare: Mapping the Cyber Underworld, Jeffrey Carr (O'Reilly Media, 2011)

[131] ...сотрудников НИИ характеризовали как «самых информированных людей в ГРУ»: «Самые информированные люди в ГРУ», доступно на [http://nvo.ng.ru/forces/2012-10-12/11\\_gru.html](http://nvo.ng.ru/forces/2012-10-12/11_gru.html)

[132] ...руководство института входит в Совет безопасности России: Указ Президента Российской Федерации от 21 января 2011 года N74 «О составе научного совета при Совете Безопасности Российской Федерации», доступно на <https://rg.ru/2011/01/23/sovbez-site-dok.html>

[133] ...Писал Стоянов... в своем открытом письме: «„Дождь“ опубликовал обращение арестованного за госизмену сотрудника „Лаборатории Касперского“», доступно на <https://meduza.io/news/2017/04/12/dozhd-opublikoval-obraschenie-arrestovannogo-za-gosizmenu-sotrudnika-laboratorii-kasperskogo>

[134] ...одним из руководителей группировки, видимо, был Максим Болонкин: «Соответствующий документ из Главного следственного управления МВД РФ по Санкт-Петербургу пришел в отдел расследований „Новой газеты“, доступно на <https://www.novayagazeta.ru/news/2014/01/31/94678-po-mestu-prozhivaniya-spikera-171-homyachkov-187-bolonkina-vzyavshego-na-sebya-otvetstvennost-za-ddos-ataki-na-sayty-smi-v-aprele-mae-2013-budet-vozbuzhdeno-ugolovnoe-delo>

[135] ...организация получила президентский грант: «За 7 млн рублей ИА „Мир“ будет нести позитив в массы», доступно на <http://sanktpeterburg.bezformata.com/listnews/mir-budet-nesti-pozitiv/26016420/>

[136] ...Содержимое взломанных почтовых ящиков Хэлл публиковал в своем блоге: <http://torquemada.bloground.ru/?p=1305>

[137] ...блог Навального взломали именно с немецкого IP: «МВД: почту Навального взломали с немецкого IP-адреса», доступно на <https://www.vedomosti.ru/politics/news/2012/08/29/mvd:-pochtu-navalnogo-vzlomali-s-nemeckogo-ip-adresa>

[138] ...Максимова арестовали немецкие полицейские по обвинению: «Что за Хэлл? В Бонне начался суд по делу о взломе российских блогов: репортаж „Медузы“», доступно на <https://meduza.io/feature/2015/06/24/chto-za-hell>

[139] ...Российских хакеров также обвиняли во взломе приложения для расчета баллистических траекторий: <https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf>

[140] ...оператор одного из центров управления энергетическими подстанциями Ивано-Франковской области заметил: Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, доступно на [https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/?mbid=nl\\_3316](https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/?mbid=nl_3316)

[141] ...В нем рассказывалось об участии российской 6-й танковой бригады: «Министр обороны РФ наградил солдат часами за Дебаль-



цево», доступно на <https://citeam.org/putin-shoygu-debaltseve/>

[142] ...Нидерландские власти использовали данные Bellingcat в расследовании: «Итоги международного расследования: „Боинг“ сбили из российского „Бука“», доступно на <https://meduza.io/feature/2016/09/28/boing-sbili-iz-rossiyskogo-buka-glavnoe>

[143] ...Ответственность за взлом взял на себя «Киберберкут»: <https://news-front.info/2016/02/24/kiberberkut-vzlomal-elektronnye-resursy-ruslana-levieva-18/>

[144] ...разобрала атаки на Левиева и Bellingcat: ThreatConnect reviews activity targeting Bellingcat, a key contributor in the MH17 investigation, доступно на <https://threatconnect.com/russia-hacks-bellingcat-mh17-investigation/>

[145] ...немецкая разведка и аналитические компании называли среди принадлежащих Fancy Bear: Pawn Storm Targets MH17 Investigation Team, доступно на <https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/>

[146] ...хакер UFO, которого вычислили спецслужбы, рассказывал: «Парень из нашего города, или „Как это бывает“», доступно на <http://xakep-archive.ru/xa/038/040/1.html>

[147] ...Источники The New York Times утверждают: Russian Espionage Piggybacks on a Cybercriminal's Hacking, доступно на [https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html?\\_r=0](https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html?_r=0)

[148] ...Бывшая сотрудница отдела кибербезопасности ФБР Милана Патель рассказывала: How To Catch A Hacker, доступно на <https://www.buzzfeednews.com/article/sheerafrenkel/inside-the-hunt-for-russias-hackers>

[149] ...В июле 2018 года в Белгороде суд прекратил уголовное дело в отношении местного жителя: «Белгородец, осуществивший хакерскую атаку на официальный сайт ФСБ, выплатит судебный штраф в размере 40 тысяч рублей», доступно на [http://oktiabrsky.blg.sudrf.ru/modules.php?name=press\\_dep&op=1&did=835](http://oktiabrsky.blg.sudrf.ru/modules.php?name=press_dep&op=1&did=835)

[150] ...Первый серьезный документ о кибервойне появился в конце 2011 года, когда Минобороны: <http://ens.mil.ru/files/morf/Strategy.doc>

[151] ...один из кураторов ГРУ, генерал Валерий Герасимов, опубликовал в журнале «Военно-промышленный курьер»: «Ценность науки в предвидении», доступно на <https://www.vpk-news.ru/articles/14632>

[152] ...вплоть до публикаций негативных отзывов на последние «Звездные войны»: «Российскую „фабрику троллей“ обвинили в разжигании споров о вреде прививок», доступно на <https://meduza.io/feature/2018/08/24/rossiyskuyu-fabriku-trolley-obvinili-v-razzhiganii-sporov-o-vrede-privivok>

[153] ...Одна из сотрудниц «фабрики» рассказывала: The Agency, доступно на <https://www.nytimes.com/2015/06/07/magazine/the-agency-russian.html>



[154] ...В одном из постов сообщалось: <https://intelligence.house.gov/uploadedfiles/6053177352305.pdf>

[155] ...американские кибервойска успешно атаковали «Агентство интернет-исследований»: U. S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms, доступно на [https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9\\_story.html?noredirect=on&utm\\_term=.80619f6afbcd](https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?noredirect=on&utm_term=.80619f6afbcd)

[156] ...сказал он на встрече с ректорами технических вузов: «Сергей Шойгу объявил о „большой охоте“ на молодых программистов», доступно

на [http://www.cnews.ru/news/top/sergej\\_shojgu\\_obyavil\\_o\\_bolshoj\\_ohote](http://www.cnews.ru/news/top/sergej_shojgu_obyavil_o_bolshoj_ohote)

[157] ...сообщил Рогозин: «В российской армии может появиться киберкомандование, заявил Рогозин», доступно на <https://ria.ru/20120321/601798789.html>

[158] ...Источники указывали, что основными задачами российских кибервойск станут «обработка информации, поступающей извне, а также борьба с киберугрозами»: «Шойгу сравнил угрозу кибербезопасности с оружием массового поражения», доступно на <https://ria.ru/20131019/971215505.html>

[159] ...Шойгу тогда повторил слова президента Владимира Путина: «Владимир Путин: Нужно усилить защиту государства от информационных атак», доступно на <https://tass.ru/politika/629732>

[160] ...в Минобороны появились «войска информационных операций»: «Источник в Минобороны: в Вооруженных Силах РФ созданы войска информационных операций», доступно на <https://tass.ru/politika/1179830>

[161] ...источники в Минобороны объяснили: «В России созданы кибервойска», доступно на <https://www.vesti.ru/doc.html?id=1573024>

[162] ...В анкете для поступления просили указать: [https://vk.com/doc-94744292\\_437246143](https://vk.com/doc-94744292_437246143)

[163] ...Новосибирский государственный технический университет объявлял среди студентов набор в научную роту: [https://www.nstu.ru/education/army\\_research](https://www.nstu.ru/education/army_research)

[164] ...при Минобороны открылась кадетская школа IT-технологий: <http://itschool.mil.ru>

[165] ...Военную академию связи окончили: «Солдаты научной роты Военной академии связи подписали первый контракт с Минобороны», доступно на [https://function.mil.ru/news\\_page/country/more.htm?id=12071767@egNews](https://function.mil.ru/news_page/country/more.htm?id=12071767@egNews)

[166] ...первые выпускники научной роты: [https://recrut.mil.ru/for\\_recruits/research\\_company/companies/7NRvas.htm](https://recrut.mil.ru/for_recruits/research_company/companies/7NRvas.htm)

[167] ...Минобороны собиралось призывать: «Рядовой хакер», доступно на <https://rg.ru/2013/07/10/roty-site.html?>



[utm\\_source=rg.ru&utm\\_medium=offline&utm\\_campaign=back\\_to\\_online](#)

[168] ...*Kremlin's ties to Russian cyber gangs sow US concerns*, доступно на <https://thehill.com/policy/cybersecurity/256573-kremlins-ties-russian-cyber-gangs-sow-us-concerns>

[169] ...кадры вирусного ролика «Я — русский оккупант»: <https://www.youtube.com/watch?v=FYy1ivz7jXQ>

[170] ...видео с сайтом *Fancy Bear*: <http://fancybear.net>

[171] ...Один из преподавателей Тамбовского учебного центра Анатолий Балюков объяснял: <http://army-today.ru/karera-i-obrazovanie/devyataya-nauchnaya/>

[172] ...Еще одна научная рота Генштаба находится в Краснодарском крае: доступно на [https://recrut.mil.ru/for\\_recruits/research\\_company/companies/6NR\\_KV\\_VU.htm](https://recrut.mil.ru/for_recruits/research_company/companies/6NR_KV_VU.htm)

[173] ...Их распорядок несильно отличается от армейского: <http://www.ulstu.ru/main?cmd=file&object=14214>

[174] ...заместитель министра обороны Юрий Садовенко рассказывал: «Заместитель министра обороны генерал-полковник Юрий Садовенко открыл новый учебный год в Рязанском высшем воздушно-десантном командном училище», доступно на [https://function.mil.ru/news\\_page/country/more.htm?id=11981620@egNews](https://function.mil.ru/news_page/country/more.htm?id=11981620@egNews)

[175] ...Минобороны сообщило: «В ходе СОУ „Щит Союза-2015“ связисты ЗВО отразили кибератаку условного противника», доступно на [https://function.mil.ru/news\\_page/country/more.htm?id=12056193@egNews](https://function.mil.ru/news_page/country/more.htm?id=12056193@egNews)

[176] ...40-серийный сериал «Ботаны»: «Капицы в погонах: один день из жизни научной роты ВКО», доступно на <https://tvzvezda.ru/news/forces/content/201411252109-vug9.htm>

[177] ...сравнивало работу научных рот с фильмами о Джеймсе Бонде: «В бой идут одни программисты», доступно на [http://army-today.ru/karera-i-obrazovanie/v-boy-idut-programmisty/?sphrase\\_id=703503](http://army-today.ru/karera-i-obrazovanie/v-boy-idut-programmisty/?sphrase_id=703503)

[178] ...Он родился в Самаре в 1920 году: «Китов Анатолий Иванович — пионер кибернетики, информатики и автоматизированных систем управления», В. А. Долгов (КОС•ИНФ, 2010)

[179] ...«Литературная газета» напечатала материал: «Кибернетика — „наука“ мракобесов?», доступно на <https://www.kp.ru/daily/22526/16560/>

[180] ...вспоминал один из студентов „спецнабора“: «Китов Анатолий Иванович — пионер кибернетики, информатики и автоматизированных систем управления», В. А. Долгов (КОС•ИНФ, 2010)

[181] ...Другой студент рассказывал: там же

[182] ...Его сын вспоминал, что идея не понравилась идеологическому отделу ЦК: «Интернет полковника Китова», доступно на [https://tvkultura.ru/brand/show/brand\\_id/59074](https://tvkultura.ru/brand/show/brand_id/59074)

[183] ...спросил кто-то американцев: <https://www.nsa.gov/Portals/70/documents/resources/everyone/di>



[digital-media-center/video-audio/historical-audio/nsa-60th/nsa-60th-1960s/19600701\\_MitchellandMartin.pdf](http://digital-media-center/video-audio/historical-audio/nsa-60th/nsa-60th-1960s/19600701_MitchellandMartin.pdf)

[184] ...перебежчиков назвали предателями и предложили расстрелять: [https://www.washingtonpost.com/opinions/nsa-secrets-revealed--in-1960/2013/06/21/35e0f072-d509-11e2-a73e-826d299ff459\\_story.html?utm\\_term=.122c9ba3b428](https://www.washingtonpost.com/opinions/nsa-secrets-revealed--in-1960/2013/06/21/35e0f072-d509-11e2-a73e-826d299ff459_story.html?utm_term=.122c9ba3b428)

[185] ...куда периодически заходил советский дипломат Валентин Иванов: «От „Ультры“ — до „Эшелона“», доступно на [https://chesspro.ru/\\_events/2009/neistadt.html](https://chesspro.ru/_events/2009/neistadt.html)

[186] ...В СССР американцы сменили имена и начали работать в НИИ: <http://documents.theblackvault.com/documents/nsa/75791A.pdf>

[187] ...в котором занимаются исследованием безопасности сетей связи: <http://ens.mil.ru/science/SRI/infrmation.htm?id=12014@morfOrgScience>

[188] ...указано на сайте НИИ: <https://www.rdi-kvant.ru/Branches.aspx/>

[189] ...В 2008 году «Квант» перешел в ведение ФСБ: <http://docs.cntd.ru/document/902053316>

[190] ...1 апреля 2011 года Бабакину пришло деликатное письмо: <https://wikileaks.org/hackingteam/emails/emailid/587613>

[191] ...Программа продавалась и продается легально за сотни тысяч долларов: <http://www.hackingteam.it>

[192] ...В другой переписке указано: <https://www.wikileaks.org/hackingteam/emails/emailid/576384>

[193] ...«Инфотекс», представляя НИИ «Квант», выплатил итальянской компании: [https://ht.transparencytoolkit.org/Amministrazione/01%20-%20CLIENTI/5%20-%20Analisi%20Fatturato/2015/02%20-%20Client%20Overview%202015/Client%20Overview\\_list\\_20150131.xlsx](https://ht.transparencytoolkit.org/Amministrazione/01%20-%20CLIENTI/5%20-%20Analisi%20Fatturato/2015/02%20-%20Client%20Overview%202015/Client%20Overview_list_20150131.xlsx)

[194] ...Позже компания заявила: «Российский заказчик Hacking Team подтвердил приобретение шпионского ПО», доступно на <https://www.forbes.ru/news/293525-rossiiskii-zakazchik-hacking-team-podtverdil-priobretenie-shpionskogo-po>

[195] ...оппозиционер Олег Козловский и сотрудник Фонда борьбы с коррупцией Георгий Албуров обвинили МТС: доступно на <https://web.archive.org/web/20160504133551/http://mts-slil.info/>

[196] ...в январе 2015 года в госизмене обвинили жительницу Вязьмы Светлану Давыдову: «„Страна больна, если шпионов ищут среди кухарок и матерей“. Как живет семья Светланы Давыдовой, которую обвиняют в госизмене», доступно на <https://meduza.io/feature/2015/01/30/strana-bolna-esli-shpionov-ischut-sredi-kuharok-i-materey>

[197] ...пытались незаконно купить микроэлектронику в США: «Научно-исследовательский институт ФСБ проводил нелегальные закупки в США», доступно на <https://www.securitylab.ru/news/442272.php>

[198] ...В одном из отчетов НИИ «Эшелон» за 2013 год: «Опыт выявления уязвимостей в зарубежных программных продуктах», до-



ступно на [https://s3r.ru/wp-content/uploads/2013/12/Kiber\\_Bezop\\_—1\\_2013\\_42.pdf](https://s3r.ru/wp-content/uploads/2013/12/Kiber_Bezop_—1_2013_42.pdf)

[199] ...почти сразу выяснилось, что 9 файлов были изменены: <https://twitter.com/BivolBg/status/860803144103723009>

[200] ...Георгий Петрович Рошка оказался сотрудником ЗАО «Эврика»: «В метаданных взломанных писем Макрона обнаружилось имя русского хакера», доступно на <https://theins.ru/politika/55118>

[201] ...Совладельцу «Эврики» принадлежит квартира: «Рошка и мышка. Почту президента Франции взломали сотрудники ГРУ», доступно на <https://theins.ru/politika/58803>

[202] ...в 2018 году обвинили в попытке атаки на Организацию по запрещению химического оружия: «Нидерланды обвинили четверых россиян в хакерской атаке. Подтвердить их связь с ГРУ может почти каждый», доступно на <https://meduza.io/slides/niderlandy-obvinili-chetveryh-rossiyan-v-hakerskoy-atake-podtverdit-ih-svyaz-s-gru-mozhet-pochti-kazhdyy>

[203] ...работали 10 хакеров: «Козачек, он же Kazak, он же blablabla1234565», доступно на <https://meduza.io/feature/2018/07/13/kozachek-on-zhe-kazak-on-zhe-blablabla1234565>

[204] ...Говорил, что обучение было похоже на «Уловку-22»: <https://mikhailmasl.livejournal.com/5591.html>

[205] ...больше половины времени отнимали лекции и семинары по математике: «О подготовке кадров в области информационной безопасности», доступно на <http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/2bc575e2571effc8c32575bd00428b4e>

[206] ...Епифанцев писал: <https://multiurok.ru/blog/proforientatsionnaia-rabota-po-podgotovkie-budushchikh-spietsialistov-v-oblasti-informatsionnykh-tiekhnologhii-dlia-silovykh-struktur-i-voienno-patriotichieskogho-vozpitanii-molodiezhi.html> (страница удалена)

[207] ...Владимир Афанасьев подтверждал, что они поддерживают проект: «Подведение итогов, презентация проекта ЦМВС МО РФ», доступно на <https://www.youtube.com/watch?v=wziNiqKpuiY>

[208] ...В подробной презентации: <https://www.slideshare.net/sergheiepifantsew5/ctf-72571006> (презентация удалена)

[209] ...«юные программисты» участвовали в конкурсе Moscow School CTF: <http://www.1770.ru/date-news/2016-12> (Страница недоступна — когда о деятельности «Юных программистов ФСБ» рассказала «Медуза», они удалили со своих сайтов и соцсетей почти все материалы)

[210] ...пришли в военной форме: [https://vk.com/album-83710188\\_238873694](https://vk.com/album-83710188_238873694)

[211] ...На сайте кадетского корпуса указано: <http://www.1770.ru/date-news/2016-12> (страница удалена)



[212] ...На главной странице была размещена его фотография на фоне герба

ФСБ: [https://lydidela.files.wordpress.com/2016/08/bn\\_wd3eijrc.jpg?w=570&h=380](https://lydidela.files.wordpress.com/2016/08/bn_wd3eijrc.jpg?w=570&h=380)

[213] ...опубликована [ссылка](#) на презентацию проекта: [https://hghltd.yandex.net/yandbtm?fmode=inject&url=https%3A%2F%2Fwww.slideshare.net%2FTCenter500%2F1770-50748329&tld=ru&lang=en&la=1494592128&tm=1495190464&text=проект юные программисты фсб россии&l10n=ru&mime=html&sign=e74453762663bde3f3188ae1c51ee5e3&keyno=0](https://hghltd.yandex.net/yandbtm?fmode=inject&url=https%3A%2F%2Fwww.slideshare.net%2FTCenter500%2F1770-50748329&tld=ru&lang=en&la=1494592128&tm=1495190464&text=проект%20юные%20программисты%20фсб%20россии&l10n=ru&mime=html&sign=e74453762663bde3f3188ae1c51ee5e3&keyno=0) (страница удалена)

[214] ...прочитал [лекцию](#) о современных войнах: <https://www.youtube.com/watch?v=s7SBGSDpRCk&feature=youtu.be> (видео удалено)

[215] ...защитивший диссертацию: доступно на <http://www.dslib.net/kult-prosvet/formirovanie-motivacii-k-voennoj-sluzhbe-u-junoshej-doprizyvno-go-vo-zrasta-v-processe.html>

[216] ...школьники [посещают](#) соревнования: доступно на [https://vk.com/album-83710188\\_237553428](https://vk.com/album-83710188_237553428)

[217] ...выступления главы Следственного комитета Александра Бастрыкина: доступно на <https://www.instagram.com/p/9bDNylhYvK/>

[218] ...фотографируются с портретом Владимира Путина: [https://vk.com/ludydela?z=photo-83710188\\_377623796%2Falbum-83710188\\_208871221%2Frev](https://vk.com/ludydela?z=photo-83710188_377623796%2Falbum-83710188_208871221%2Frev) (фотография удалена)

[219] ...Также они [переводили](#) книгу про американского хакера: «Шкворень: школьники переводят книгу про хакеров», доступно на <https://habr.com/ru/post/261491/>

[220] ...получают десятки грамот: <https://fsb.ru.com/%20наши-достижения/> (страница удалена)

[221] ...один из учеников в августе 2015 года [удостоился](#) нагрудного знака: <https://multiurok.ru/blog/naghrazhdeniie-znakom-fsb-rf.html> (страница удалена)

[222] ...весной 2017 года они [сняли](#): <https://www.youtube.com/watch?v=eYPPRKKKvp4> (видео удалено)

[223] ...который [представляли](#) на базе ЦСКА: <https://www.instagram.com/p/BTOIMNFgbga/?taken-by=itcoder> (пост удален)

[224] ...Один из них [заканчивается](#) кадром: <https://www.youtube.com/watch?v=26zTC8eDmzE> (видео удалено)

[225] ...До кадетского корпуса он [работал](#) заместителем директора специального интерната: «Дети боевого братства», доступно на <https://www.youtube.com/watch?v=cBrr9kcnQY0>

[226] ...На сайте департамента образования Москвы [указано](#): [https://sch1770.mskobr.ru/common\\_edu/moskovskij\\_kadetskij\\_muzy](https://sch1770.mskobr.ru/common_edu/moskovskij_kadetskij_muzy)



[kal\\_nyj\\_korpus/obwie\\_svedeniya/pedagogicheskij\\_kollektiv/uchitelya\\_matematiki\\_i\\_informatiki/epifancev\\_sergej\\_vladimirovich/](http://kal_nyj_korpus/obwie_svedeniya/pedagogicheskij_kollektiv/uchitelya_matematiki_i_informatiki/epifancev_sergej_vladimirovich/)

[227] ...в хакерском коде были фрагменты на кириллице: Dark Territory: The Secret History of Cyber War, Fred Kaplan (Simon & Schuster, 2017)

[228] ...В еженедельнике Newsweek вышел материал «Мы находимся на кибервойне»: We're In The Middle Of A Cyerwar, доступно на <https://www.newsweek.com/were-middle-cyerwar-166196>

[229] ...а одно из писем исправил пользователь «Феликс Эдмундович»: Commentary: Don't be so sure Russia hacked the Clinton emails, доступно на <https://www.reuters.com/article/us-russia-cyberwar-commentary-idUSKBN12X075>

[230] ...Пресс-секретарь Владимира Путина Дмитрий Песков заявлял: «Песков: Россия не причастна к атаке хакеров на американские базы данных», доступно на <https://www.vesti.ru/doc.html?id=2765084>

[231] ...Управление директора национальной разведки США опубликовало доклад: Background to «Assessing Russian Activities and Intentions in Recent US Elections»: The Analytic Process and Cyber Incident Attribution, доступно на [https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf)

[232] ...Fancy Bear за 2015 год отправили минимум 4400 фишинговых писем: <https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf>

[233] ...были выложены документы ВАДА: «Хакеры атаковали ВАДА», доступно на <https://meduza.io/feature/2016/09/13/hakery-atakovali-vada>

[234] ...эксперты указывали: <https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf>

[235] ...среди серверов — те, что располагаются в России: A Voice Cuts Through, and Adds to, the Intrigue of Russia's Cyberattacks, доступно на [https://www.nytimes.com/2016/09/28/world/europe/russia-hacker-vladimir-fomenko-king-servers.html?\\_r=0](https://www.nytimes.com/2016/09/28/world/europe/russia-hacker-vladimir-fomenko-king-servers.html?_r=0)

[236] ...при атаке на иранскую ядерную программу, использовалось четыре уязвимости нулевого дня: «Холодная хакерская война У Агентства национальной безопасности США, кажется, украли кибероружие», доступно на <https://meduza.io/feature/2016/08/17/holodnaya-hakerskaya-voyna>

[237] ...Для работы с похожими уязвимостями, видимо, набирали специалистов в Центр специальных разработок Минобороны: «Минобороны РФ ищет специалистов по реверс-инжинирингу», доступно на <https://news.softodrom.ru/ap/b19249.shtml>

[238] ...группировка не совершала «коммерческих взломов»: <https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf>

[239] ...«Лаборатория Касперского» еще в 2014 году рассказывала о группировке APT28: The CozyDuke APT, доступно на <https://securelist.com/the-cozyduke-apt/69731/>



[240] ...В судебных документах было подробно изложено: <https://www.justice.gov/file/1080281/download>

[241] ...Согласно документам американских спецслужб, подполковник Сергей Моргачёв командовал подразделением воинской части: «В США предъявили обвинения 12 сотрудникам ГРУ по делу о вмешательстве в выборы», доступно на <https://meduza.io/news/2018/07/13/v-ssha-pred-yavili-obvineniya-12-sotrudnikam-gru-po-delu-o-vmeshatelstve-v-vybory>.

[242] ...она давала показания по этому делу на слушаниях в конгрессе: «11 часов допроса», доступно на <https://meduza.io/feature/2015/10/23/11-chasov-doprosa>

[243] ...The New York Times писала, что ключевую помощь в поиске хакеров американским спецслужбам оказали источники в России: Top Russian Cybercrimes Agent Arrested on Charges of Treason, доступно на <https://www.nytimes.com/2017/01/25/world/europe/sergei-mikhailov-russian-cybercrimes-agent-arrested.html>

[244] ...там появилась радикальная группировка, преследовавшая гомосексуалов: «Образцово-показательное унижение», доступно на <https://lenta.ru/articles/2013/07/05/kamenskursky/>

[245] ...вспоминал он: «Лицом к лицу с хакером», доступно на <https://www.vedomosti.ru/newspaper/articles/2004/11/02/licom-k-licu-s-hakerom>

[246] ...О себе он подробно рассказывал на своем сайте (сейчас удален): <https://web.archive.org/web/20050410043421/http://kamensk.net.ru:80/forb/info/common/my.html>

[247] «Я на диване (1997 год)»: <https://web.archive.org/web/20050421230800/http://kamensk.net.ru:80/forb/cgi-bin/foto.cgi?area=me&num=1>

[248] ...переехал в Москву и стал работать в «Хакере» как штатный сотрудник: «История журнальных компьютерных хулиганов», доступно на <https://xakep.ru/2007/12/04/x-history-1999-2007/>

[249] ...неизвестные записали заседания на диктофон, а потом выложили в открытый доступ: <https://soundcloud.com/5qlw9z0f2kxa/15-08-2017>

[250] ...такой случай действительно был 8 августа 2013 года: «Взломанный твиттер РИА Новости сообщил о смерти Горбачева», доступно на <https://lenta.ru/news/2013/08/08/ria/>

[251] ...например, на американскую АЭС: IAEA chief: Nuclear power plant was disrupted by cyber attack, доступно на <https://uk.reuters.com/article/us-nuclear-cyber-idUKKCN12A10C>

[252] ...узнать об этом можно из исследования научно-производственного объединения «Эшелон»: «Организационно-технические проблемы защиты от целевых вредоносных программ типа STUXNET», доступно на [https://s3r.ru/wp-content/uploads/2013/12/Kiber\\_Bezop\\_—1\\_2013\\_28.pdf](https://s3r.ru/wp-content/uploads/2013/12/Kiber_Bezop_—1_2013_28.pdf)

[253] ...В июле 2016 года ФСБ сообщила об обнаружении троянов в информационной инфраструктуре правительственных, научных и обо-



ронных учреждений страны: «ФСБ выявила вирус для кибершпионажа в сетях 20 госорганов и предприятий ОПК», доступно на <https://tass.ru/ekonomika/3498890>

[254] ...Под каждое предприятие писался свой эксплойт: «За чиновниками шпионили через web-камеры», доступно на [https://www.gazeta.ru/tech/2016/07/30\\_a\\_9720437.shtml](https://www.gazeta.ru/tech/2016/07/30_a_9720437.shtml)

[255] ...В парламентском комитете по безопасности тогда заявили: там же

[256] ...хакеры годами атакуют российские военные ведомства: «Эксперты обнаружили атаку хакеров на военно-промышленный комплекс России», доступно на [https://www.rbc.ru/technology\\_and\\_media/08/02/2018/5a7c3ee29a79471c93ab30b3](https://www.rbc.ru/technology_and_media/08/02/2018/5a7c3ee29a79471c93ab30b3)

[257] ...российские чиновники используют закрытую государственную сеть: [http://www.tadviser.ru/index.php/Статья: Единая\\_сеть\\_передачи\\_данных\\_\(ЕСПД\)\\_для\\_госорганов\\_\(Russian\\_State\\_Network,\\_RSNet\)](http://www.tadviser.ru/index.php/Статья:Единая_сеть_передачи_данных_(ЕСПД)_для_госорганов_(Russian_State_Network,_RSNet))

[258] ...выпустил «криптотелефон»: [http://stcnet.ru/products\\_iid\\_17.htm](http://stcnet.ru/products_iid_17.htm)

[259] ...Российский аналог американского Агентства национальной безопасности, ФАПСИ, появился в начале 1990-х: «Internet тотального контроля», доступно на <https://www.kommersant.ru/doc/14591>

[260] ...Владимир Маркоменко во время выступления в Госдуме в 1996 году говорил: «Вызовы в сфере информационной безопасности: оценка актуальности угроз», доступно на <http://studies.agentura.ru/listing/vyzovi/>

[261] ...Сотрудник ведомства рассказал: «Интервью с сотрудником ФАПСИ», доступно на <http://xakep-archive.ru/xa/046/050/1.htm>

[262] ...Как писал журналист The New York Times Дэвид Сэнгер: Obama Order Sped Up Wave of Cyberattacks Against Iran, доступно на <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>

[263] ...Источники указывали, что Stuxnet создали спецслужбы: <http://www.zerodaysfilm.com/>

[264] ...пецслужбы сначала атаковали пять иранских компаний: An Unprecedented Look at Stuxnet, the World's First Digital Weapon, доступно на <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

[265] ...23 июня 2017 года газета The Washington Post рассказала: Obama's secret struggle to punish Russia for Putin's election assault, доступно на [https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?pushid=594cf6ea2e12651d00000094&tid=notifi\\_push\\_breaking-news&utm\\_term=.cff22297a4f4](https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?pushid=594cf6ea2e12651d00000094&tid=notifi_push_breaking-news&utm_term=.cff22297a4f4)

[266] ...бывший директор АНБ и ЦРУ Майкл Хайден говорил: <http://www.zerodaysfilm.com>

[267] ...Еще в конце 1990-х чеченские террористы атаковали российские государственные ресурсы и СМИ: «Вызовы в сфере инфор-



мационной безопасности: оценка актуальности угроз», доступно на <http://studies.agentura.ru/listing/vyzovi/>

[268] ...*ISIS Hacking Division* или «Киберхалифат»: Inside the hacker underworld of ISIS, доступно на <https://www.businessinsider.com/isis-hacking-division-operates-2016-6>

[269] ...У Трика к тому времени был большой опыт: свой первый взлом он совершил в 11 лет: там же

[270] ...В 2012 году после взлома почты помощника бывшего премьер-министра Великобритании Тони Блэра: The Curious Case of the Jihadist Who Started Out as a Hacktivist, доступно на <https://www.vanityfair.com/news/2015/12/isis-hacker-junaid-hussain>

[271] ...Например, в январе 2015 года Хуссейн разместил в твиттере американского центрального военного командования пост: Ex-TeaMp0isoN Leader «TRiCk» Linked to Hackers Taking Over @CENTCOM, доступно на <https://news.softpedia.com/news/Ex-TeaMp0isoN-Leader-Trick-Linked-to-Hackers-Taking-Over-CENTCOM-470094.shtml>

[272] ...оказался на третьем месте в списке Пентагона на уничтожение: British hacker is No 3 on Pentagon «kill list», доступно на <https://www.thetimes.co.uk/article/british-hacker-is-no-3-on-pentagon-kill-list-6g95bfqwfznz>

[273] ...после смерти Трика он написал: <https://imgur.com/b1t98pl>

[274] ...Он утверждал, что помог спецслужбам из-за того, что те угрожали его семье: Hacker Outs Himself as FBI «Snitch» and Claims He Helped Track Down ISIS, доступно на [https://motherboard.vice.com/en\\_us/article/nz7w9b/hacker-outs-himself-as-fbi-snitch-and-claims-he-helped-track-down-isis](https://motherboard.vice.com/en_us/article/nz7w9b/hacker-outs-himself-as-fbi-snitch-and-claims-he-helped-track-down-isis)

[275] ...эту информацию подтверждает один из отчетов Group-IB: <https://www.group-ib.ru/resources/threat-research/2016-report.html>

[276] ...уже многие годы различные группировки ищут красную ртуть: The Doomsday Scam, доступно на <https://www.nytimes.com/2015/11/22/magazine/the-doomsday-scam.html>

[277] ...Владимир Путин поручил ФСБ создать государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак: Указ Президента Российской Федерации от 15 января 2013 г. N31с г. Москва «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», доступно на <https://rg.ru/2013/01/18/komp-ataki-site-dok.html>

[278] ...2015 году ФСБ опубликовала выписку из нее: [http://www.fsb.ru/files/PDF/Vipiska\\_iz\\_koncepcii.pdf](http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf)

[279] ...ведомственные центры реагирования уже запустили Центробанк и «Ростех»: «„Ростех“ занялся парированием киберугроз», доступно на <https://iz.ru/news/642771>

[280] .....Новиков объяснял, что сейчас спецслужбы выстраивают обмен информацией об инцидентах: «BIS TV — НКЦКИ: Состояние и перспективы развития (Алексей Новиков) — IX Уральский форум», доступно на <https://www.youtube.com/watch?v=c7gOPOFBQX0>



[281] ...говори́лось в пояснительной записке ФСБ к законопроекту: [http://asozd.duma.gov.ru/addwork/scans.nsf/ID/EBE024490F4C5851432580810054D3AC/\\$File/47571-7\\_06122016\\_47571-7.PDF?](http://asozd.duma.gov.ru/addwork/scans.nsf/ID/EBE024490F4C5851432580810054D3AC/$File/47571-7_06122016_47571-7.PDF?OpenElement)

[OpenElement](#)

[282] ...Владимир Путин называл эту же цифру, говоря о 2015 годе: «Владимир Путин выступил на коллегии ФСБ», доступно на <https://www.1tv.ru/news/2015-03-29/22210-vladimir-putin-vystupil-na-kollegii-fsb>

[283] ...объяснял Шальков, представляя законопроект в Госдуме: доступно на <http://www.video.duma.gov.ru/watch/?id=310933>

[284] ...В первом чтении его приняли 27 января 2017 года: доступно на [http://asozd2.duma.gov.ru/main.nsf/\(SpravkaNew\)?OpenAgent&RN=47571-7&02](http://asozd2.duma.gov.ru/main.nsf/(SpravkaNew)?OpenAgent&RN=47571-7&02)

[285] ...глава ФСБ Александр Бортников попросил депутатов ускорить принятие законопроектов о критической инфраструктуре: «Глава ФСБ попросил Думу ускорить принятие законов о регулировании в Сети», доступно на <https://www.rbc.ru/politics/23/06/2017/594ceb609a7947265009bfc8>

[286] ...вместе с ним приняли поправку к закону о гостайне: «Информационной инфраструктуре придали критическую скорость», доступно на <https://www.kommersant.ru/doc/3344780>

[287] ...Технический директор «Роскомсвободы»: «Российские власти хотят изолировать интернет. Теперь у нас будет как в Китае?», доступно на <https://meduza.io/feature/2018/12/17/rossiyskie-vlasti-hotyat-izolirovat-internet-teper-u-nas-budet-kak-v-kitae>

[288] ...Средства для защиты критической инфраструктуры выпускают многие коммерческие компании: <https://www.ptsecurity.com/ru-ru/products/isim/>, <https://www.group-ib.ru/tds.html>, [https://media.kaspersky.com/pdf/Kaspersky\\_Industrial\\_CyberSecurity\\_brochure.pdf](https://media.kaspersky.com/pdf/Kaspersky_Industrial_CyberSecurity_brochure.pdf)

[289] ...Журнал Forbes сообщал, что «Информзащита» за пять лет заключила четыре с половиной сотни контрактов: «Посторонних нет: как создавался бизнес по охране государственных секретов», доступно на <http://www.forbes.ru/kompanii/internet-telekom-i-media/314311-postoronnikh-net-kak-sozdavalsya-biznes-po-okhrane-gosudars>

[290] ...средство защиты сетей и шифровки данных «Континент», которое используется многими: [https://www.securitycode.ru/company/news/kompaniya\\_informzashchita\\_poluchila\\_novyy\\_sertifikat\\_fsb\\_rossii\\_na\\_apksh\\_kontinent/](https://www.securitycode.ru/company/news/kompaniya_informzashchita_poluchila_novyy_sertifikat_fsb_rossii_na_apksh_kontinent/)

[291] ...С «Информзащитой» среди прочих работала Алиса Шевченко: «Еще одна маленькая девочка-хакер», доступно на <https://meduza.io/feature/2016/12/30/esche-odna-milenkaya-devochka-haker>

[292] ...В своем инстаграме Шевченко называла себя «еще одной миленькой девочкой-хакером»: <https://www.instagram.com/alisaesage/?hl=ru>



[293] ...Шевченко начинала свою карьеру, работая вирусным аналитиком: «Еще одна маленькая девочка-хакер», доступно на <https://meduza.io/feature/2016/12/30/esche-odna-milenkaya-devochka-haker>

[294] ...как указывал Forbes, они занимались разработкой инструментария для взломов: «Контракт со взломом: как хакер построила бизнес за счет банков и корпораций», доступно на <https://www.forbes.ru/tekhnologii/internet-i-svyaz/275355-kontrakt-na-ugrozu-kak-khaker-stroit-biznes-na-zashchite-bankov>

[295] ...Власти США считают, что компания Шевченко предоставляла свои исследования и разработки ГРУ: FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment, доступно на <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and>

[296] ...сайт ее компании перестал открываться: <http://zorsecurity.ru>

[297] ...Тогда они уверяли, что смогли получить разработку: «Холодная хакерская война», доступно на <https://meduza.io/feature/2016/08/17/holodnaya-hakerskaya-voyna>

[298] ...Президент Microsoft... сравнил случившееся с потенциальной кражей крылатых ракет «Томагавк»: The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack, доступно на <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/>

[299] ...Делфи вспоминал: He Perfected a Password-Hacking Tool — Then the Russians Came Calling, доступно на <https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/>

[300] ...Спецслужбы США и Великобритании заявили: White House blames Russia for «reckless» NotPetya cyber attack, доступно на <https://ca.reuters.com/article/technologyNews/idCAKCN1FZ2UJ-OCATC>

[301] ...Заместитель секретаря Совбеза РФ Олег Храмов говорил: «Угрозы информационной безопасности становятся все более изощренными и масштабными», доступно на <https://www.kommersant.ru/doc/3303788>

[302] ...указано в отчете: «Эхо кибервойны», доступно на <https://www.group-ib.ru/blog/wannacryptor>

[303] ...немецкий исследователь информационной безопасности Тобиас Энгель показал собравшимся способы слежки за абонентами: Locating Mobile Phones using Signalling System #7, доступно на <https://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf>

[304] ...в других американских документах такие атаки упоминались еще с 1998 года: Here's Why Anyone Could Hack Your Phone, доступно на <https://www.thedailybeast.com/heres-why-anyone-could-hack-your-phone>



[305] ...В том же году The Washington Post рассказала: New documents show how the NSA infers relationships based on mobile location data, доступно на [https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/?utm\\_term=.fbfee6aede3b](https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/?utm_term=.fbfee6aede3b)

[306] ...журналисты издания сообщили о специальных программах для слежки: For sale: Systems that can secretly track where cellphone users go around the globe, доступно на [https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f\\_story.html?utm\\_term=.8ae6beff86b1](https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html?utm_term=.8ae6beff86b1)

[307] ...с помощью SS7 хакеры могут «определить местоположение абонента в любой точке мира: German researchers discover a flaw that could let anyone listen to your cell calls, доступно на <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/>

[308] ...но преступные группировки берут оборотом: «Атака хакеров: как пропадают миллиарды», доступно на <https://hbr-russia.ru/biznes-i-obshchestvo/fenomeny/a16348/>

[309] ...получив доступ к SS7, хакер может перехватить коды авторизации: «Как взломать Telegram и WhatsApp: спецслужбы не нужны», доступно на <https://habr.com/ru/company/pt/blog/283052/>

[310] ...говорил немецкий хакер Карстен Нол: Cell Phone Network Flaws Can Help Spies Get Around Encryption Apps, доступно на [https://motherboard.vice.com/en\\_us/article/78k4vb/cell-phone-network-flaws-can-help-spies-get-around-encryption-apps](https://motherboard.vice.com/en_us/article/78k4vb/cell-phone-network-flaws-can-help-spies-get-around-encryption-apps)

[311] ...Согласно исследованию американской компании FireEye: <https://www2.fireeye.com/rs/fireeye/images/rpt-m-trends-2015.pdf>

[312] ...взломе своих аккаунтов в Telegram сообщили оппозиционер Олег Козловский и сотрудник Фонда борьбы с коррупцией Георгий Албуров: [https://web.facebook.com/kozlovsky/posts/10208948934790884?\\_rdc=1&\\_rdr](https://web.facebook.com/kozlovsky/posts/10208948934790884?_rdc=1&_rdr)

[313] ...В службе поддержки ему якобы заявили: <https://soundcloud.com/kozlovsky/mts-otb>

[314] ...представитель МТС Дмитрий Солодовников сообщил: «МТС опроверг „целенаправленное“ отключение SMS оппозиционерам во время взлома Telegram», доступно на <https://meduza.io/news/2016/04/29/mts-oproverg-tselenapravlennoe-otklyuchenie-sms-oppozitsioneram-vo-vremya-vzloma-telegram>

[315] ...Верховный суд России признал законным право спецслужб прослушивать оппозиционеров: «Верховный суд поддержал прослушку оппозиционеров», доступно на <https://republic.ru/posts/l/864280>



[316] ...В расследовании российского Forbes указывалось: «Колпак для оппозиции: как советская система прослушки возродилась в России», доступно на <https://www.forbes.ru/tehnologii/231333-kolpak-dlya-oppozitsii-kak-sovetskaya-sistema-proslushki-vozrodilas-v-rossii>

[317] ...Якеменко и Потупчик решили собрать группу людей: <https://lj.rossia.org/users/kremlingate/?skip=20>

[318] ...Василий Якеменко сначала открыл кафе «Ешь пирог», потом занялся книжным клубом: «Печатный станок: как Василий Якеменко создал финансовую пирамиду на книгах», доступно на [https://tvrain.ru/teleshov/bremja\\_novostej/yakemenko-431316/](https://tvrain.ru/teleshov/bremja_novostej/yakemenko-431316/)

[319] ...купил дом в Баварии: <https://twitter.com/yakemenko/status/219393783568146432>

[320] ...назначил мне встречу в любимом месте выходцев из движения «Наши»: «Боты — новые солдаты», доступно на <http://mag.afisha.ru/stories/realnosti-ne-sushestvuet/boty-novye-soldaty/>

[321] ...согласились пообщаться со мной: «Мы делаем то, что нам велит наша совесть», доступно на <https://daily.afisha.ru/archive/gorod/archive/anonymous-russia/>

[322] ...хакеры также взломали сайт калужского отделения «Единой России»: «Взломщики почты Якеменко пригрозили разоблачениями „продажным блоггерам и чиновникам“», доступно на <https://www.newsru.com/russia/08feb2012/anon.html>

[323] ...Все в итоге получили сроки: «Хакер вне политики», доступно на <https://www.kommersant.ru/doc/2375565>

[324] ...Параллельно активисты опубликовали: «Обращение Anonymous к гражданам России», доступно на <https://www.youtube.com/watch?v=zGVnZShlZ1E>

[325] ...Роскомнадзор располагается в восьмиэтажном здании на Китай-городе: «Как устроен Роскомнадзор», доступно на <https://meduza.io/feature/2015/03/13/kak-ustroen-roskomnadzor>

[326] ...Уже через два месяца этот закон внеесли в Госдуму: [http://asozd2.duma.gov.ru/main.nsf/\(Spravka\)?OpenAgent&RN=553424-6](http://asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=553424-6)

[327] ...обязал хранить все записи звонков: «„Пакет Яровой“ принят больше полугода назад. Как он работает?», доступно на <https://meduza.io/feature/2017/02/13/zakon-yarovoy-prinyat-bolshe-polugoda-nazad-kak-on-rabotaet>

[328] ...К 2017 году Роскомнадзор каждый день в среднем блокировал 244 страницы в интернете: «Основная мишень — пользователи», доступно на <https://meduza.io/feature/2018/02/05/osnovnaya-mishen-polzovateli>

[329] ...Они написали: [https://twitter.com/Russian\\_Revolt/status/444364017608720384](https://twitter.com/Russian_Revolt/status/444364017608720384)

[330] ...Они рассказывали о взломе антидопингового агентства WADA: Anonymous Russia — Fancy Bears Operation Olympics, доступно на [https://www.youtube.com/watch?v=BSgxms6Lz\\_U](https://www.youtube.com/watch?v=BSgxms6Lz_U)



[331] ...документы о том, как компания Евгения Пригожина «Конкорд» курирует кремлевских «интернет-троллей»: «Сотни троллей за миллионы», доступно на <https://www.fontanka.ru/2014/05/29/170/>

[332] ...зеркальный сайт: <http://b0ltay.blogspot.com/>

[333] ...выложили предполагаемую переписку вице-премьера Аркадия Дворковича: «Аркадий Дворкович стал жертвой хакеров», доступно

на <https://www.vedomosti.ru/politics/articles/2014/07/22/arkadij-dvorkovich-postupil-v-rassylku>

[334] ...Через месяц «Анонимный интернационал» рассказал о трех почтовых ящиках Дмитрия Медведева: <https://www.rbc.ru/society/14/08/2014/570420ae9a794760d3d40b3f>

[335] ...«Шалтай» слил электронную переписку аффилированной с московским правительством компании: «Хакеры опубликовали переписку СМИ о проплаченных предвыборных статьях», доступно на <https://www.novayagazeta.ru/news/2014/09/24/105893-hakery-opublikovali-perepisku-smi-o-proplachennyh-predvybornyh-statyah>

[336] ...опубликована предполагаемая переписка замначальника секретариата: <https://meduza.io/news/2014/10/30/v-set-popala-perepiska-zamnachalnika-sekretariata-igorya-shuvalova>

[337] ...с сумкой, набитой деньгами: «Анонимный интернационал: „Потупчик получила в АП не менее 15 миллионов“», доступно на <https://theins.ru/politika/2230>

[338] ...он обсуждал заказные материалы против Алексея Навального: «Письма Администрации президента: как заказали Навального», доступно на <https://theins.ru/politika/2349>

[339] ...Шалтай и Болтай утверждали, что публикуют сливы, потому что их «не устраивают ограничение свободы»: «Неравнодушные люди сами виноваты, что потеряли интернет», доступно на <http://www.lookatme.ru/mag/people/manifesto/206757-shaltay-boltay>

[340] ...Своей целью «Анонимный интернационал» объявлял: «„Мы не маленькие дети в этом бизнесе“: „Шалтай-Болтай“ — о своих последних сливах», доступно на <https://apparat.cc/world/boltai/>

[341] ...Один из членов группировки цитировал фильм «Хранители»: <https://web.archive.org/web/20141105174535/http://spektr.delfi.lv/novosti/my-ne-slivaem-my-rasskazyvaem-pravdu.d?id=45161768>

[342] [https://meduza.io/image/attachments/images/000/003/340/large/nP615dSOj6V6WzHF6\\_RWSQ.jpg](https://meduza.io/image/attachments/images/000/003/340/large/nP615dSOj6V6WzHF6_RWSQ.jpg)

[343] ...потом — с «Дождем» в Таллине: «Сооснователь „Шалтая-Болтая“ — Собчак: „ФСБ обещала гарантировать нам безопасность“», доступно на [https://tvrain.ru/teleshow/sobchak\\_zhivem/shaltai-427271/](https://tvrain.ru/teleshow/sobchak_zhivem/shaltai-427271/)



УДК 004.491

ББК 60.54

T86

Туровский, Даниил.

Вторжение. Краткая история русских хакеров / Даниил Туровский. — Москва: Индивидуум, 2019. — 296 с.

ISBN 978-5-6042627-3-3

Летом 2016 года неизвестные выложили в интернет переписку высших чинов Демократической партии США — и российские хакеры, предположительно работающие на Кремль, моментально превратились в один из главных сюжетов мировой политики. Спецкор «Медузы», обладатель премии GQ в номинации «Журналист года» и четырех премий «Редколлегия» Даниил Туровский к тому времени писал об этих людях уже несколько лет: одни из них публиковали архивы почты российских чиновников, другие взламывали госсайты сопредельных стран по просьбе спецслужб, третьи просто зарабатывали миллионы, воруя их по всему миру. «Вторжение» — самая полная история российских хакеров: от советских матшкол и постсоветской нищеты к мировой кибервойне и транснациональным преступным группировкам. Книга описывает новый тип власти — но, как показывает Туровский, люди, которые обладают этой властью, сталкиваются все с теми же моральными дилеммами, выбирая между тюрьмой и сумой, чувством и долгом, добром и злом.

© Туровский, Д., 2019

© ООО «Индивидуум Принт», 2019

Даниил Туровский

Вторжение.

Краткая история русских хакеров

18+

Издатели: Андрей Баев, Алексей Докучаев

Главный редактор: Феликс Сандалов

Арт-директор: Максим Балабин

Редактор: Александр Горбачев

Корректоры: Мария Москвина, Надежда Власенко

Редакция благодарит Павла Грозного за помощь в продюсировании книги

ООО «Индивидуум Принт»

[indiviumbooks.ru](http://indiviumbooks.ru)

[info@indiviumbooks.ru](mailto:info@indiviumbooks.ru)

[facebook.com/indiviumbooks](https://facebook.com/indiviumbooks)

[instagram.com/indivium\\_books](https://instagram.com/indivium_books)

Подписано в печать 18.04.19